NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USING WIRELESS SENSOR NETWORKS IN IMPROVED EXPLOSIVE DEVICE DETECTION

by

Joshua Sundram
Phua Poh Sim

December 2007

Thesis Co-Advisors: Gurminder Singh
Neil C. Rowe

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Using Wireless Sensor Networks in Improvised Explosive Device Detection	**5. FUNDING NUMBERS**
6. AUTHOR(S) Joshua Sundram; Phua Poh Sim	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research focused on wide-area surveillance of public environments for potential IEDs (improvised explosive devices) using wireless sensor networks. We explored magnetic and infrared sensors from Crossbow Technologies to detect simulated emplaced IEDs (emplacement is the step most susceptible to detection) in a public mall and along a typical street environment. The threat scenario was IED emplacement in a trash receptacle. A network of these sensors was built and positioned in these environments with human subjects entering (some carrying ferromagnetic materials and some not) and proceeding toward a receptacle. Results indicated that magnetic sensors could detect suspicious ferromagnetic materials, though not all simulated IEDs contained enough to trigger detection. Infrared sensors were not effective for such tasks as there is much background infrared radiation. Our network design was such that data could easily be aggregated over many sensors in larger networks. This suggests that the technology can be effective for protecting communal areas such as airports and urban areas. Other supplementary technologies such as imagery could be linked to build a more robust detection network.

14. SUBJECT TERMS wireless sensor networks (WSN), improvised explosive devices (IED), crossbow, magnetic, infrared, test	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

USING WIRELESS SENSOR NETWORKS IN IMPROVISED EXPLOSIVE DEVICE DETECTION

Joshua Sundram
Major, Singapore Armed Forces (Army)
B.Eng. (E.E), Nanyang Technological University, 2002

Phua Poh Sim
Captain, Singapore Armed Forces (Army)
B.Eng. (Mech), Imperial College London, 2001
M.Phil (Operational Research), University of Cambridge, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Authors: Joshua Sundram

Phua Poh Sim

Approved by: Gurminder Singh, PhD
Thesis Co-Advisor

Neil C. Rowe, PhD
Thesis Co-Advisor

Peter J. Denning, PhD
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research focused on wide-area surveillance of public environments for potential IEDs (improvised explosive devices) using wireless sensor networks. We explored magnetic and infrared sensors from Crossbow Technologies to detect simulated emplaced IEDs (emplacement is the step most susceptible to detection) in a public mall and along a typical street environment. The threat scenario was IED emplacement in a trash receptacle. A network of these sensors was built and positioned in these environments with human subjects entering (some carrying ferromagnetic materials and some not) and proceeding toward a receptacle. Results indicated that magnetic sensors could detect suspicious ferromagnetic materials, though not all simulated IEDs contained enough to trigger detection. Infrared sensors were not effective for such tasks as there is much background infrared radiation. Our network design was such that data could easily be aggregated over many sensors in larger networks. This suggests that the technology can be effective for protecting communal areas such as airports and urban areas. Other supplementary technologies such as imagery could be linked to build a more robust detection network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our utmost gratitude to Prof Singh and Prof Rowe for their dedication in providing valuable advice and time for the past months; without which the timely completion of this thesis would not have been possible. We would also like to thank Donna Dulo for her tireless efforts in helping us understand how Crossbow sensors work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. IMPROVISED EXPLOSIVE DEVICE (IED) THREATS

Improvised-explosive devices (IEDs) are “homemade” bombs containing conventional military explosives, such as trinitrotoluene (TNT), and/or common household substances such as ammonium nitrate (garden fertilizer), attached to a detonator and an initiating mechanism. The classification of IEDs is usually by their delivery means; typical classifications include vehicle-borne IEDs (VIEDs), packaged IEDs (PIEDs) and roadside bombs. IED threats are particularly difficult for militaries to assess and resolve in spite of the recent research across the security spectrum. “The IED continues to be the single largest threat that coalition forces face in Iraq; there were 11784 known IED-related incidents in 2004” [12]. Usually considered a form of asymmetric offense, IED incidents can result in significant fatalities and collateral damage and are becoming the weapons of choice for the terrorist groups and insurgents. IEDs can be devastating weapons due to their ease of targeting state assets such as soldiers, government officials, transportation infrastructure, and aid vehicles.

The effectiveness of IEDs has impaired many coalition operations in Iraq and Afghanistan. To date IEDs in Iraq alone have claimed more than 1500 lives and injured many thousands [3]. IEDs have proven to be highly effective unconventional weapons, yet inexpensive for the adversary to build and deploy. It is reported that about $6.1 billion has been spent on U.S. efforts to defeat IEDs [26]. But current countermeasures have only been partially effective despite of these multi-billion expenditures.

The deployment of IEDs involves several tasks ranging from motivation to funding to emplacement and detonation. While legislative controls such as denying access to precursor chemicals used to manufacture explosives [17] may potentially disrupt the IED life cycle, a popular approach to defeating IEDs lies with emplacement detection. However, such detection is a challenging task when they are buried, and is difficult even when they are above ground.

B. WORK ON IED DETECTION

There has been extensive research on IED detection using handheld devices, unmanned ground vehicles, and unmanned aerial vehicles. Research has employed a myriad of signature-based detection schemes, behavioral disparity, and so on; even mine dogs (Warfighter IED Conference, 2005) are beginning to gain popularity as potential efficient IED detection tools. We can classify these detection techniques or equipment as being active or passive. Active detection means stimulating a response from explosives or the device using radiation such as x-rays or radio frequencies. Passive detection means trace detection such as vapor or microscopic elements emitted from the explosives. The following detection schemes are limited to already-emplaced IEDs.

1. Passive Detection

Chemiluminescence (emission of light without emission of heat) used for the detection of IEDs, exploits "detection of infrared light emitted from electronically-excited NO_2 chemical compositions which most explosives contain" [4]. This technique possesses good sensitivity when used in combination with high-speed gas chromatography and can detect a wide range of explosives such as DNT (dinitrotoluene), RDX (cyclotrimethylene-trinitramine) and PETN (pentaerythritol tetranitrate).

A chemical signature-based detection technique with a vapor sensor "Fido" [28] is used with the "Dragon Runner" robotic platform (see Figure 1). It is reported that this system can detect a wide range of IEDs, even those concealed in vehicles. However, there still exist employability issues, such as "the need for a sensor algorithm that alerts the operator with an alarm," as well as the need for "ruggedization."

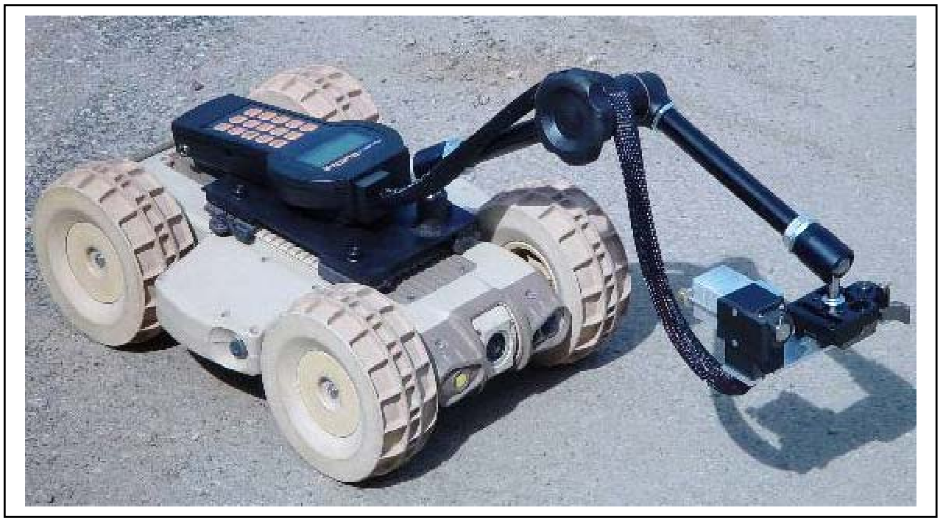


Figure 1. Fido XT deployed on the Dragon Runner (from Ref. [28]).

Another approach is a combination of magnetic sensors and a UAV which uses the magnetic properties that are contained in most unexploded ordnance and IEDs (most of which contain steel). As described in [34], “magnetic sensors are configured as a tensor magnetic gradiometer that detect magnetic targets using magnetic moments.” Platforms other than UAVs could be also used to fulfill the objective of a wide coverage.

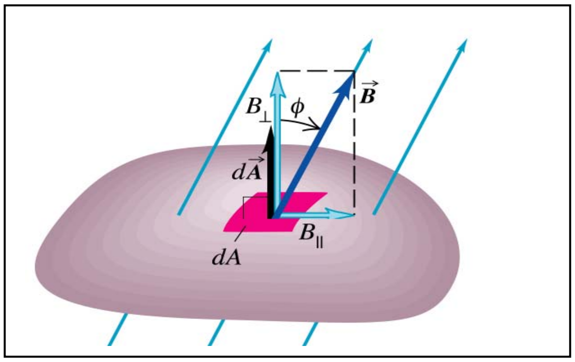


Figure 2. Depiction of magnetic flux through an area element *d*A (from Ref. [34]).

There are several commercial detection systems (comprised of a suite of sensors such as magnetic and chemical) but they are limited in utility primarily due to the lack of accuracy, sensitivity and false alarm rates. This could be attributed to a high dependency of IED signatures on environmental conditions which complicate data collection and performance assessment, particularly in a suburban to urban environment.

2. Active Detection

MMW radiometers are sensors used for monitoring soil moisture and other geophysical data. [38] proposes using MMW radiometers to detect signatures from disturbed soil and vegetation stress that are caused by buried IEDs; images of buried IEDs can be constructed by using “MMW active illumination” method.

Another approach is a nuclear detection system where thermal low-energy neutrons detect explosive materials. “Neutrons have excellent penetrating power and interact with nitrogen-rich materials, such as explosives, in a well-known and predictable way” [4]. This detection technique is based on the release of wavelength-specific gamma ray photons when a thermal neutron is absorbed by nitrogen compounds present in explosives such as TNT and C4.

There is also ongoing research to develop chemical sensors through a variety of techniques. One interesting development is “advanced nanostructured miniature explosives sensors with high sensitivity and fast response” [29]. It uses a molecular mechanics analysis using Chem3D (a core application of ChemOffice used for modeling and visualization) to locate ideal host molecules to bond with IED targets.

C. MOTIVATION

Our thesis attempts to address the detection of the action of IED emplacement. Detection of emplaced explosive devices is difficult as they can be concealed to remain undetectable by many kinds of sensors. This problem is still more difficult when IEDs are emplaced in crowded areas where there exist numerous interferences. Our thesis will investigate the feasibility of an implementation of a modular wireless sensor network to detect emplaced IEDs. The experimentation will use a sensor system from Crossbow

Technologies. It is hoped that with a suitable topology and modular configuration of these wireless sensors, greater accuracy can be obtained. This may potentially reduce public concerns and services disruptions at places like airports and train stations by minimizing first-response actions such as area cordoning and crowd dispersal, as well as reduce fatalities in conflict-infested areas of operations.

D. OBJECTIVES

The purpose of the thesis is to evaluate a sensor network comprising passive infrared and magnetic sensors in the detection of emplacement of IEDs in suburban to urban environments. Our objectives are:

1. Characterization of IEDs (constituents, emplacement and triggering techniques, and emplacement environments).

2. Investigation and recommendation of an efficient topology (positioning) of sensor nodes for effective IED detection in a controlled test environment.

3. A proof-of-concept demonstration of the feasibility of adopting a wireless sensor network comprising of magnetic and passive infrared sensors to isolate and detect emplacement of IEDs in publicly accessible receptacles, i.e. trash bins, postal boxes, etc.

E. THESIS ORGANISATION

Chapter II provides background on IEDs, past and current research, and sensors used for IED detection and identification. Chapter III presents our experimental methodology including the variables to be investigated, test scenarios based on actual IED occurrences, and the employment of sensors. Chapter IV presents the experimental results. Chapter V presents the findings from the results and provides an analysis (identification of limitations or weaknesses which could be reinforced) of these findings. Chapter VI presents the conclusion and proposes recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IMPROVISED EXPLOSIVE DEVICES AND SENSOR NETWORKS

A. IED CHARACTERISTICS

IEDs, commonly known as "homemade bombs," are used almost exclusively by rogue entities with the intent of achieving an asymmetric tactical advantage over the adversary. The DOD-NATO definition is “a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract; it may incorporate military stores, but is normally devised from nonmilitary components.” They are bombs much like mines and implemented in an improvised manner to destroy or incapacitate personnel or vehicles [10]. IEDs are usually command-detonated and are emplaced with specific targets and windows of opportunity in mind (as offensive in nature). Mines, on the other hand, are often used in defensive postures such as border defense, denial of access to main supply routes, etc. and are triggered by pressure or a tripwire (non-command detonation). IEDs are typically composed of an explosive charge, a detonator, and an initiating system. They are difficult to detect in part due to the myriad of packaging techniques afforded to the bombmaker. However some generalizations are possible which will aid IED detection.

1. Common Constituents

a. Main Charge

While there are many types and forms of munitions, PE4, TNT, ammonium nitrate (common garden fertilizer), and fuel oil (ANFO) are some of the common military and commercial explosives used in IEDs. Objects such as nails, ball bearings (also known as shipyard confetti after the metal waste found in the shipyards of Belfast), bolts, common hardware, and propane and fuel tanks are often used to enhance the fragmentation and thermal effects [5, 10]. Most IEDs use conventional high-explosive charges as their payload. However, toxic chemical, biological, or radioactive material could be added to the device, creating other life-threatening effects beyond shrapnel, concussive blasts and fire usually associated with bombs.

b. Initiating System

An initiating system typically consists of a firing device or switch (electric or non-electric), an initiator (usually a blasting cap), and a power source (batteries) if an electric initiation is used [10, 12]. Initiating systems (triggers) can include cell phones, walkie-talkies, or anything that will receive a radio or electronic signal. Non-electric systems are usually based on pressure or tripwire actuation.

c. Casing

The casing or container which houses the IED can be anything ranging from carcasses, cigarette packets, drink cans, or paving materials to a large truck or airplane. Its purpose is to conceal the IED and to provide fragmentation if possible.

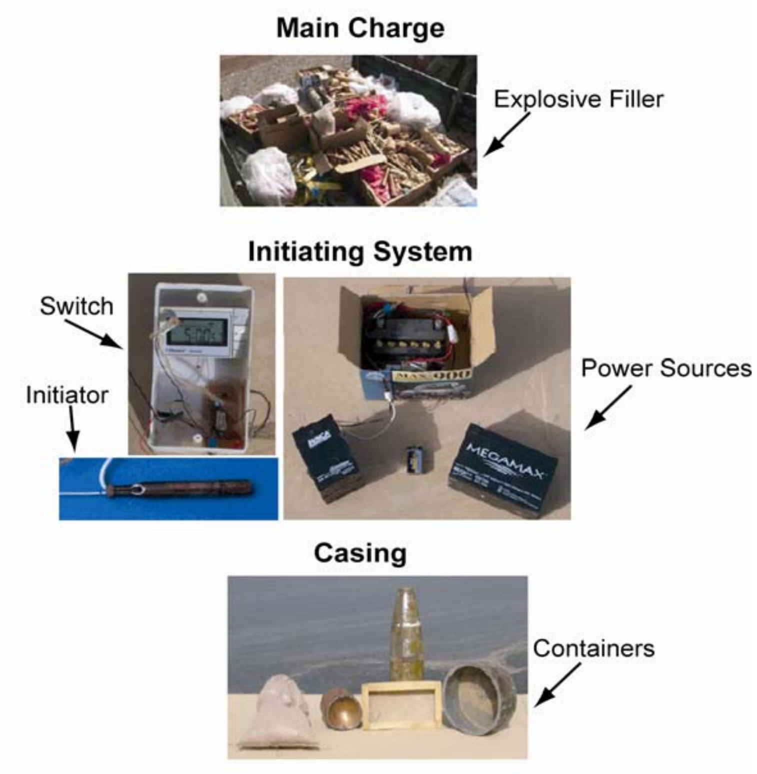


Figure 3. Components of an IED (from Ref. [10]).

2. Initiation Methods

There are two primary initiation methods, instantaneous and delayed [10]. Triggering for IEDs may include using commercial electronics or may even be as simple as running over a rubber hose to produce enough air pressure to activate a switch. Some IEDs have been remotely detonated with radio frequencies using simple readily available low-technology devices such as car alarms, key fobs, door bells, cellular telephones and pagers. Remote detonation requires observation of the target area and probably line-of-sight observation points, but with some standoff ability to watch forces from a distance and not be compromised.

The most popular initiation method is the command detonated/initiated method [11]. This allows the adversary the choice of the optimum moment of initiation. It is normally used against targets that are in transit or where a routine pattern has been established. The most common forms are wireless, wired, and voice-communication activation.

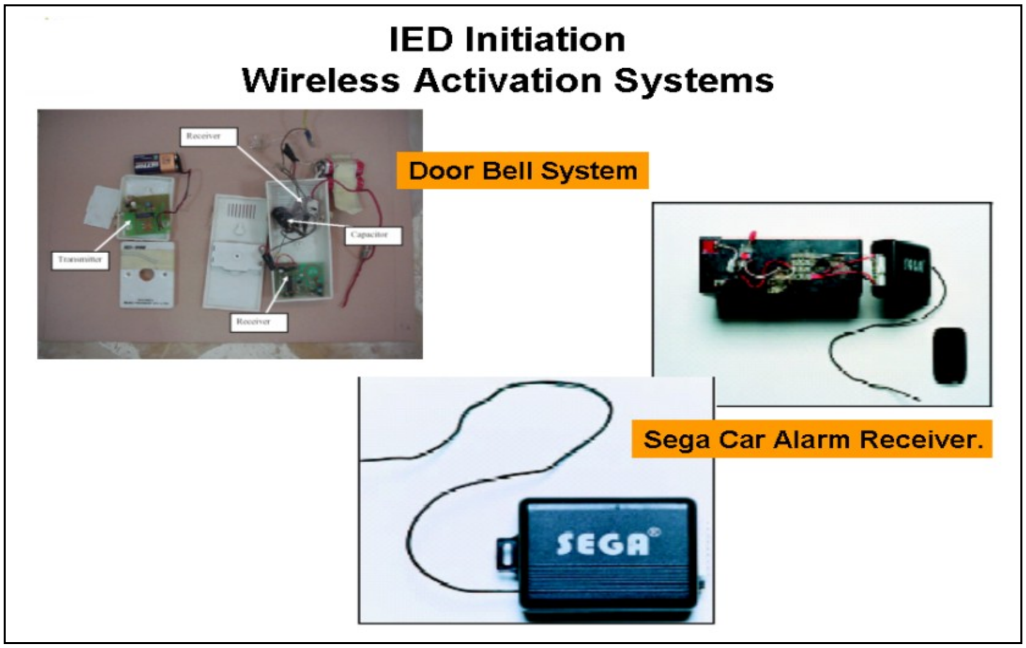
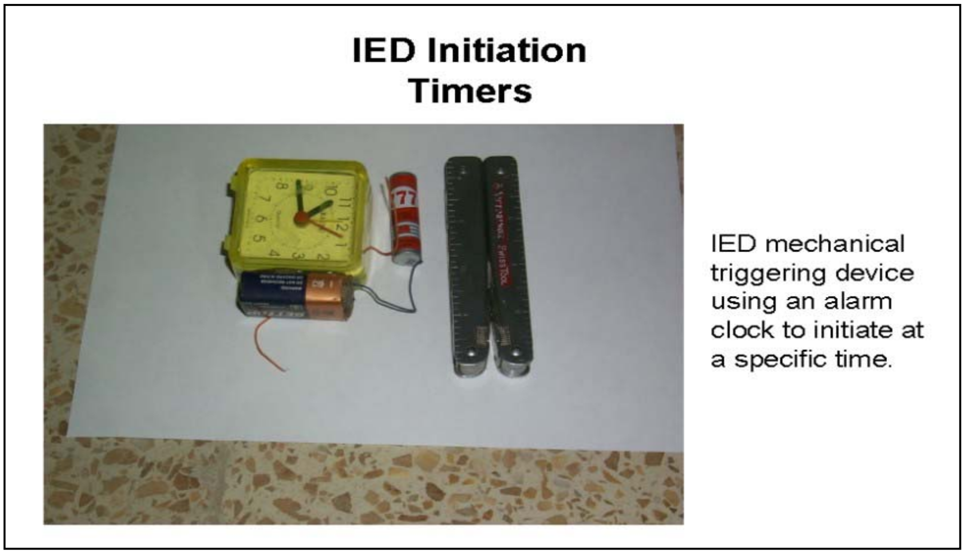

IED Initiation
Wireless Activation Systems

Figure 4. Wireless activation system (from Ref. [15]).

Time-delayed devices are designed to operate after a preset time. This affords the adversary the advantage of being at a far distance at the time of attacks but requires a somewhat accurate prediction of time and route that a target will traverse.



IED Initiation Timers

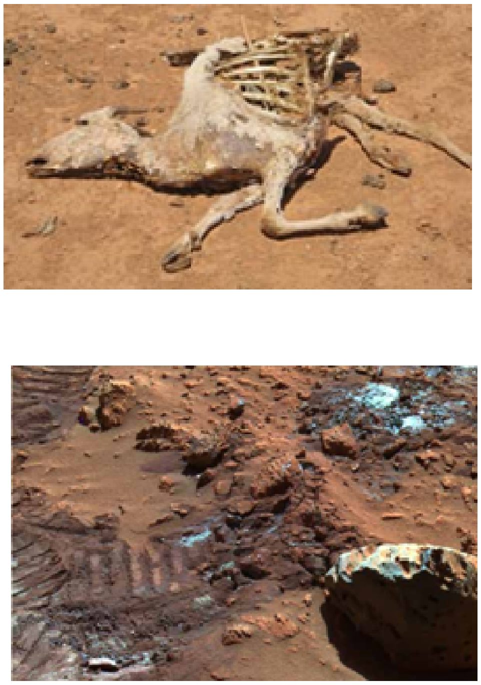
IED mechanical triggering device using an alarm clock to initiate at a specific time.

Figure 5. IED Timer system (from Ref. [15]).

3. Indicators

The indicators of emplaced IEDs are somewhat similar to those of conventional booby traps. (The DOD-NATO definition is “an explosive or nonexplosive device or other material deliberately placed to cause casualties when an apparently harmless object is disturbed or a normally safe act is performed.”) They are usually visual, such as disturbed soil and sand, isolated boxes and containers along common roads, or exposed trip wires, strings or cables left behind by the perpetrators intentionally or accidentally. These indicators include both physical and behavioral irregularities. While it is easier said than done, most military personnel are taught to look for such telltale signs; increased vigilance does increase the possibility of IED detection. Examples [10] of indicators include, but are not limited to:

- Personnel on overpasses
- Signals from vehicles and/or bystanders
- Suspicious objects such as unattended containers
- Markers by the roadside serving as possible aiming references
- Graffiti or writings on buildings
- Disturbances of the ground surface or scattered, loose soil
- Improvised methods of marking such as piles of stones or marks on walls or trees
- Metallic objects such as drink cans and cylinders
- Videotaping of seemingly ordinary activities or military activities
- Unusual behavioral patterns such as the absence of women and children, or a noticeably reduced number of vehicles or people in a normally busy period or area



Animal carcass

Disturbed ground

Figure 6. IED Indicators (from Ref. [15]).

4. Employment Techniques and Targets

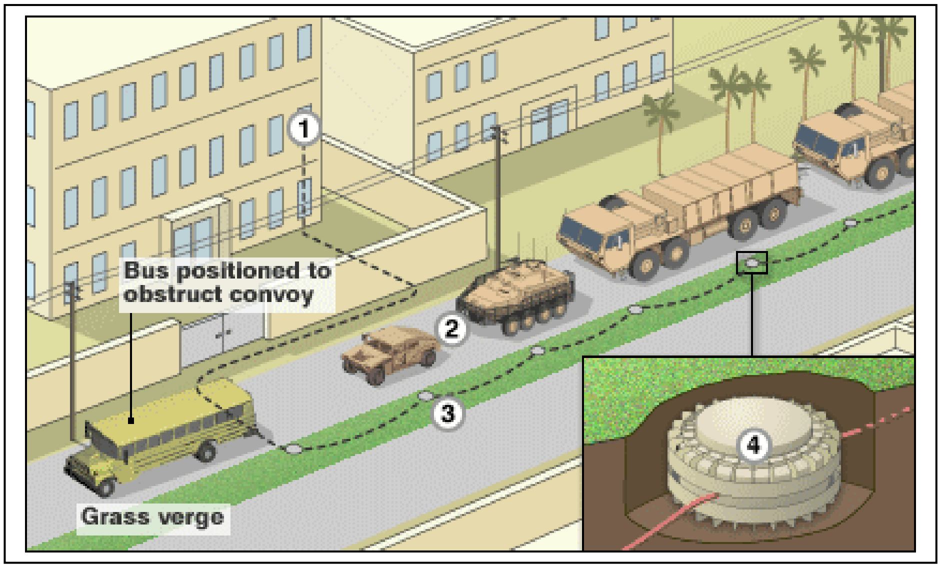
IEDs are often characterized by their employment techniques. A mine or explosive is often used, but unexploded ordnance can be easily engineered to replace them.

- Buried mines can be stacked on top of one another to increase the force of a blast. Coupling is a method of linking one mine or explosive device to another, to expand the area covered by explosions [10, 11]. Anti-personnel mines may be used in daisy chains linked with other explosive hazards (Figure 7). Mines may be linked together with trip wire or detonating cord. When the initial mine is detonated, other mines may detonate either sympathetically or by design. This creates large lethal engagement areas.

- "To foil devices on the fronts of vehicles using rollers and other methods to trigger early detonation, the IED can be designed so the roller will pass over the initial, unfuzed device and set off the second fuzed device."[11] This can in turn detonate an overpassed device underneath the clearing vehicle. When the linked devices are directional fragmentation mines, they can create a large engagement area.

- On some anti-tank mines, the pressure plate can be cracked and the spring is removed to reduce the pressure required to initiate the mine [5]. A pressure-fuzed antipersonnel mine can be placed on the top of an antitank mine, thus creating a very large mine as an alternative method.

- A patrol can be attacked with IEDs, inflicting casualties. When first responders arrive to help, other pre-placed bombs can be triggered to those personnel, or a follow-on attack can be begun with rifles or grenades.



1. Hidden perpetrator with detonator watching the road. **2. Coalition convoy.**

3. IEDs buried in grass verge linked by 'daisy-chaining'. **4. Anti-tank mines used as IED.**

Figure 7. Depiction of a typical IED daisy-chaining (from Ref. [15]).

- Typical targets of IED are those of high visibility (including those of high exposure to media) or high value, as well as military targets. Lines of communications are particularly popular targets due to their frequent, sometimes inevitable, use by friendly forces due to the mobility requirements for troop replenishment and other logistical requirements. Bridges and overpasses present excellent vantage points for IEDs nearby. Checkpoints and control points which are critical junctions are also viewed as valued targets.

5. Locations

IEDs can be emplaced almost anywhere there is sufficient space for concealment and there are possible vantage points for the usual line-of-sight activations. However IEDs are most likely to be emplaced along main routes such as supply routes that are heavily used by friendly forces. In recent years in Iraq and Afghanistan, IEDs are commonly emplaced in urban to suburban areas such as shopping malls, religious infrastructure, roadsides paralleling government agencies [3], etc. as part of asymmetrical tactics commonly used in low intensity conflicts. The IEDs are often activated during peak hours to inflict the most casualties. Common IED locations are:

- Past successful emplacements
- Trees, lampposts, overpasses, and bridge spans
- Checkpoints or regulatory points
- Animal carcasses
- Buildings
- Roadway shoulders and road craters (in asphalt layers, dirt tracks, etc.)
- Frequently traveled routes like patrol routes

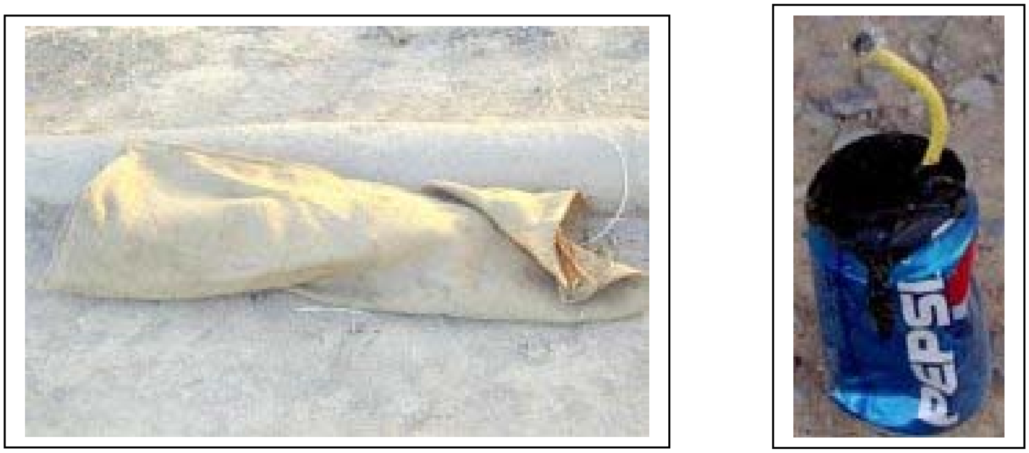
B. GENERAL CATEGORIZATION OF IEDS

IEDs vary based on the type of explosive used, method of assembly, and the method of detonation. The following are some of the general categories of IEDs.

1. Packaged IED (PIED)

A PIED may be hastily camouflaged with dirt, rocks, trash or items that are commonly found on or alongside roads. These devices can either be detonated by wire, a remote control device, or a combination of both. The ease of concealing explosives in packages or containers of various forms and sizes suggests that there are literally no obvious limits on PIEDs' sizes and thus the extents of damage - depending upon the intended targets and damages to be inflicted, PIEDs' sizes can range from a small beverage can to something larger such as an artillery shell (Figure 8).

PIEDs have been used in both conventional and non-conventional contexts such as main supply routes, and shopping malls and other communal environments respectively. Increasingly, vehicles are equipped with armor so as to counteract the explosive effects of PIEDs emplaced along critical supply route. To that end, explosively formed penetrators (EFPs) have been used in PIEDs against these armored cars; an EFP is a special type of shaped charge designed to penetrate armor effectively at stand-off distances. The use of EFPs in PIEDs poses an even greater threat due to their penetration prowess which inflicts direct bodily harm to the vehicle’s crew [5].



Artillery shell-based IED hidden in bags **Drink can**

Figure 8. Examples of packaged IEDs (from Ref. [18]).

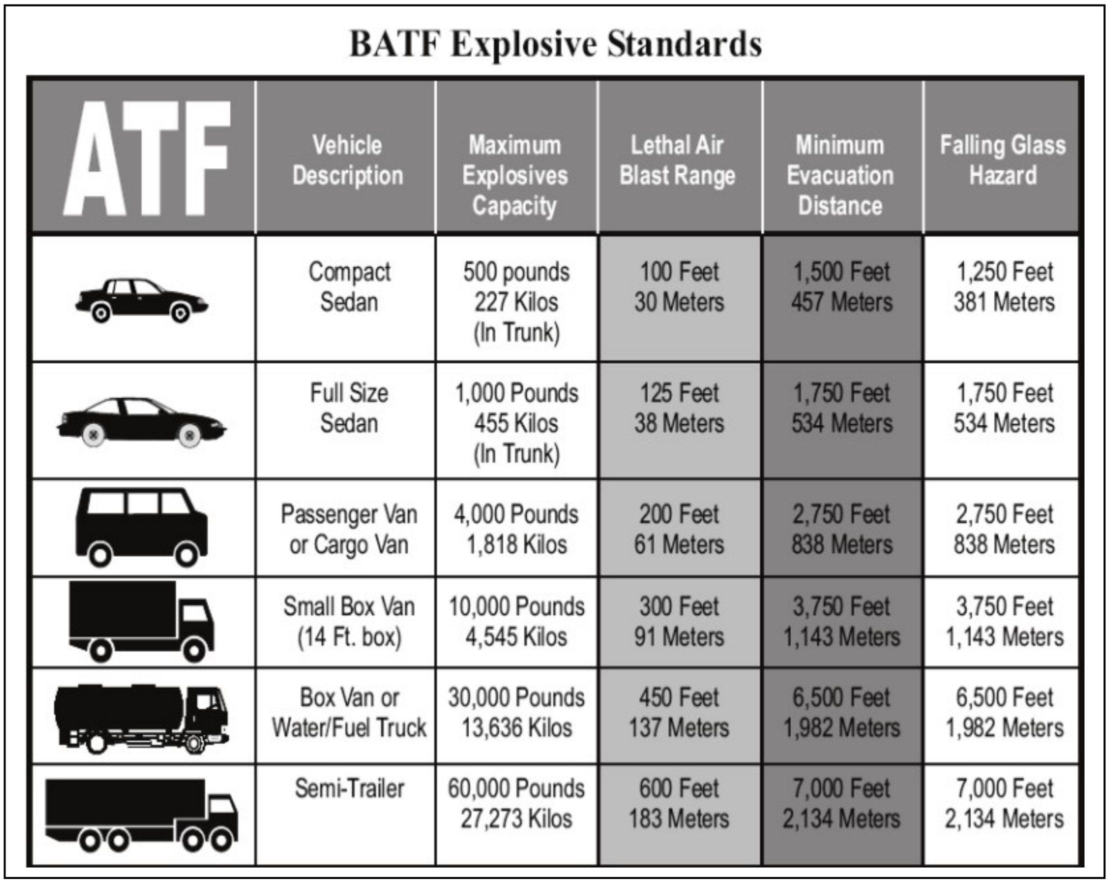
2. Vehicular IED (VIED)

A VIED is one of the most common forms of suicide bombing where the perpetrator conceals an explosive device in a vehicle; a vehicle-assisted attack offers the opportunity for mass casualties [13]. An example of VIED attack was the World Trade Center attack in New York in 1993, carried out with rented vehicles carrying an estimated 1200 pounds of explosives. Some of the common applications of suicide VIEDs include:

- Broken-down car/truck – the VIED is parked along a known route and the perpetrator appears to be fixing a tire or repairing an engine problem, and the VIED is detonated as the target comes into range.
- Single suicide VIED – the bomber pulls up alongside of the target, either at a stop or speeds up to ensure target is within the blast radius.
- Multi-suicide VIED – multiple VIEDs execute the same techniques and procedures as above.

- Suicide VIED detonation against a complex or facility.

As 9/11 has seen, a VIED is not restricted to wheeled or static platforms; aircraft or other mobile platforms are used as well. Table.1 shows the amount of explosives that each category of vehicles can carry and their associated minimum evacuation distances. These classifications are particularly useful for area cordoning and crowd dispersal when there are suspicious vehicles nearby. These distances may also provide government contractors a useful template for erecting security checkpoints or bollards.



BATF Explosive Standards

ATF	Vehicle Description	Maximum Explosives Capacity	Lethal Air Blast Range	Minimum Evacuation Distance	Falling Glass Hazard
	Compact Sedan	500 pounds 227 Kilos (In Trunk)	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	Full Size Sedan	1,000 Pounds 455 Kilos (In Trunk)	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	Passenger Van or Cargo Van	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	Small Box Van (14 Ft. box)	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	Box Van or Water/Fuel Truck	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,500 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	Semi-Trailer	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

Table 1. U.S. Bureau of Alcohol, Tobacco and Firearms (BATF) vehicle-bomb explosion and evacuation-distance table.

3. Suicide Bombers

Common terms for suicide tactics include martyrdom operations, genocide bombings, suicide bombings and suicide attacks. So far there is “no official government definition of suicide terrorism” [6]. Suicide attacks are generally inexpensive but highly effective. It is estimated that it costs as little as $150 to conduct a suicide attack or bombing [12], albeit a certain amount of detailed planning has to be conducted. While media coverage is common, another key objective of suicide attacks is to garner sympathy and allow romanticization of the act which may aid in recruitment [2]. Perpetrators of suicide attacks are usually associated with PIEDs and VIEDs. Such acts are usually harder to prevent than other IEDs as they are non-static as compared to emplaced VIEDs and PIEDs.

4. IED Operational Structure

IED organizational structures are small and typically consist of six to eight personnel, ranging from “bombmakers,” “emplacers” to “triggermen” [7]. These operatives are usually ex-military personnel adept with basic military operations. The bombmakers are usually skilled at bomb-making. Even if unskilled, they can easily obtain these skills from other IED cells and via the internet. The emplacer is the one who undertakes the highest risk of positioning the IEDs at targeted locations at specific times, often traveling along high-trafficked roads frequently patrolled by law-enforcement agencies. The triggerman is responsible for detonating the IEDs at an opportune time to inflict the greatest damage on the targets. Common detonating means include wireless and wired activations using accessories such as cell phones and common household wires respectively. While it is essential to attack the entire IED delivery structure, it is most feasible to disrupt the IED cycle by apprehending the emplacer; hence the significance of research using WSN (employing various sensors) to detect emplacement of IEDs.

C. TRENDS IN IED OCCURRENCES

In the recent conflicts in Iraq and Afghanistan, IED attacks have had destabilizing and destructive effects on coalition operations. From July 2003 to September 2007, there have been 1626 IED-related casualties on the coalition forces in Iraq alone. This shows why IEDs are likely to be a serious world problem in coming years. In general, an increasing trend in IED-caused fatalities is suggested by Figure 9.

Table 2 shows IED occurrences by the environments that these IED were found in Iraq and Afghanistan. There are three primary categories of environments: city squares, roadsides or streets, and confined spaces (which include train stations, airports, shopping malls, and places of worship).

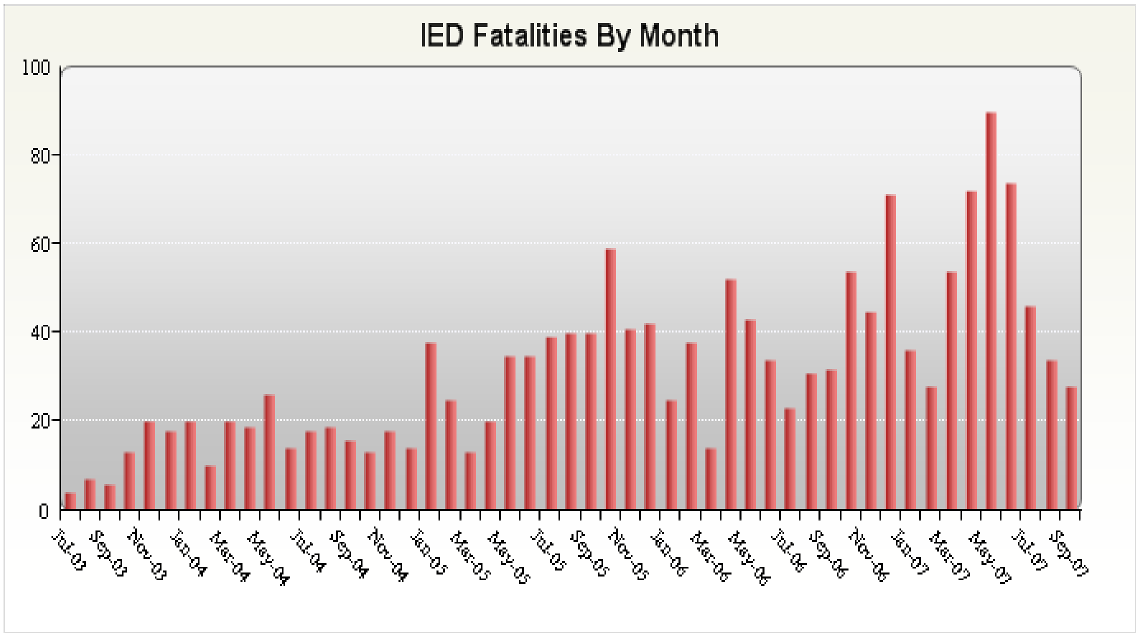


Figure 9. IED fatalities in Iraq by month (from Ref. [16]).

City Squares	**Roadsides / Streets**		**Confined Spaces**	
44	Government buildings	103	Train stations	22
	Others	65	Airports	34
	subtotal	**168**	Shopping malls	32
			Places of worship	75
			subtotal	**163**
Total: **375**				

Table 2. Tabulation of media-reported IED occurrences from Jun 2006-2007.

Typical environments in which IED occurrences have been reported are urban-to-suburban terrains and these terrains are complex. Urban areas provide advantages to insurgents and terrorists [22], in both combat and non-conventional operations, because of the asymmetric benefits of the civilian population and infrastructure. Simulating them will be important in the test environments where we will be conducting experiments. The three main kinds of urban environments (see Figure 10) we need to address in experiments are:

City Squares

- High volume of human and vehicular traffic
- Plentiful avenues of approach
- Restricted freedom of vehicular movement and maneuver
- Degraded communications due to limited lines of sight
- Identifiable traffic patterns (i.e. rush hours, weekends, day/night hours)
- Identifiable background infrared and magnetic signatures
- Containers such as trash bins and mail boxes at fixed known locations

Roadsides / Streets

- High volume of human and vehicular traffic
- Restricted avenues of approach (particularly with blockades)
- Restricted freedom of vehicular movement and maneuver
- Degraded communications due to limited lines of sight
- Identifiable traffic patterns (i.e. rush hours, weekends, day/night hours)
- Identifiable background infrared and magnetic signatures
- Containers such as trash bins and mail boxes at fixed known locations
- Usually lined with parked vehicles
- Essential buildings such as financial houses, embassies, other government agencies, etc.

Confined spaces

- Identifiable human traffic patterns (i.e. festivals, holiday or off-peak seasons, and rush hours)
- Restricted avenues of approach (exits and entrances)
- Identifiable background infrared and magnetic signatures
- Existence of containers such as trash bins and mail boxes at fixed known locations
- May include parked vehicles if parking spaces are available

Figure 10. Sample pictures of typical IED environments (from Ref. [14]).

D. WIRELESS SENSOR NETWORKS

1. Introduction to Wireless Sensor Networks

A wireless sensor network (WSN) is a collection of sensor nodes that are organized into a cooperative network [19]; they are ad-hoc systems containing sensors connected by wireless links. Wireless sensor networks have numerous applications, ranging from habitat monitoring to environmental control [27], and in the military realms of intelligence, surveillance and reconnaissance (ISR) or "surveillance and battle-space monitoring" [23]. A broad overview of wireless sensors networks is presented in [9].

a. Utility of Sensor Networks in ISR

Sensor networks (wireless in particular) can alert command-and-control units of events of interest such as presence of unusual personnel and/or objects (such as vehicles and suspicious packages). ISR missions often entail a high degree of risk to personnel. Hence unmanned systems such as sensors are of practical importance to the military for handling missions such as nuclear attacks, biological attacks, chemical attacks, and reconnaissance.

This suggests that the detection of IEDs could benefit from wireless sensors networks. Increasingly wireless sensors are used to cooperatively detect and identify targets of interest, alert more powerful sensors to capture video and audio data, and deliver the aggregated data to command-and-control units with long-range communication devices. Figure 11 is a conceptual depiction of an interagency cooperative structure using wireless sensor networks for command and control. For example, sensor nodes picking up suspicious activities will forward the data via repeaters to relay stations. These relay stations then notify backend operators / analysts, whom may activate necessary services such as the rescue teams, fire brigades and law enforcement agencies.

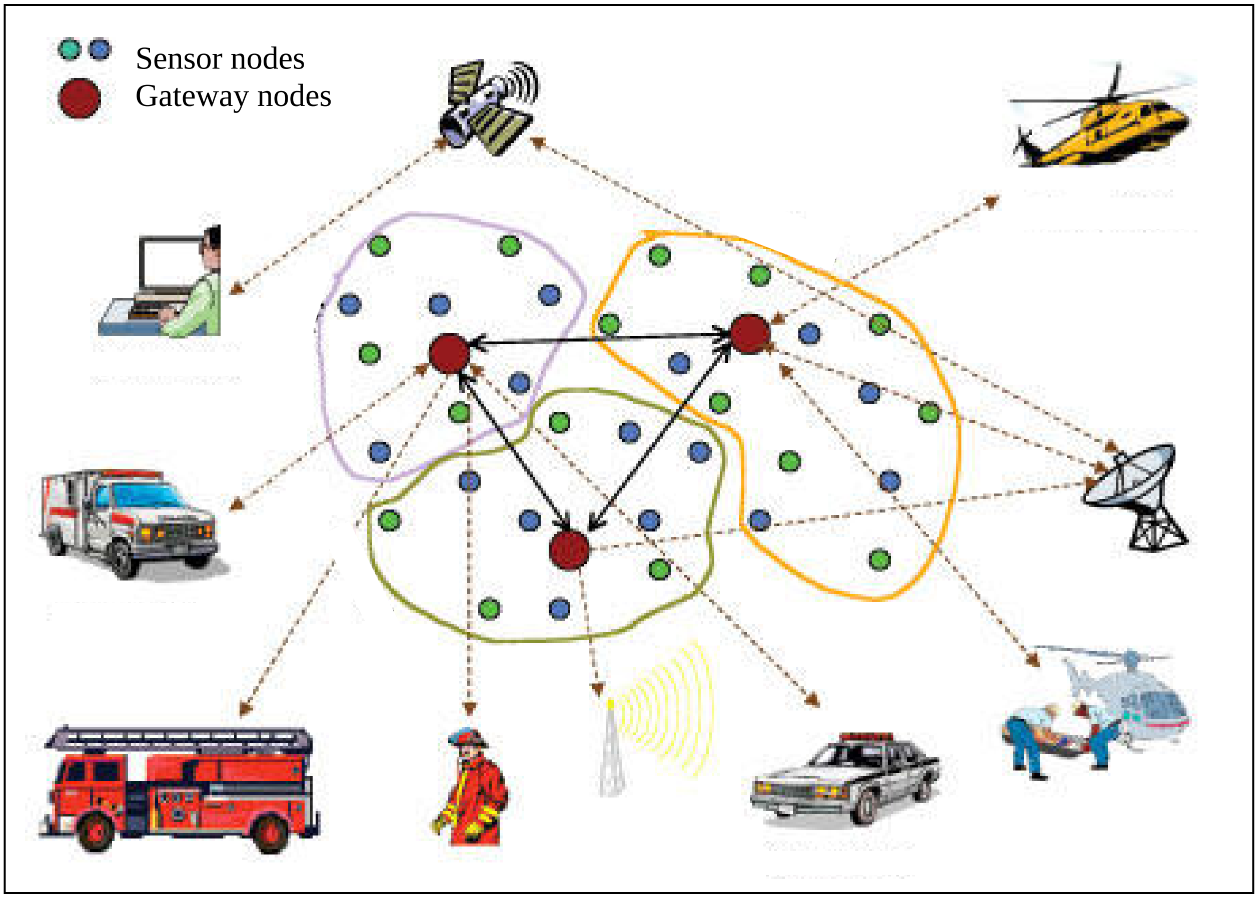


Figure 11. Depiction of wireless sensor network applications and the possible interoperability between different agencies (from Ref. [14]).

b. Characteristics of WSN

While there are many characteristics associated with wireless sensor networks as outlined by [9, 20], characteristics important to IED detection are:

- Minimal intrusiveness (especially when sensors are sited in public areas such as shopping malls and airports);
- Distributed data collection (permitting self-healing when a node failure occurs);

- Energy efficiency (necessary to maintain as long an operational life as possible, particularly when regular battery renewal is infeasible);
- Security (sensor nodes are usually sited in accessible areas, risking of physical sabotage);
- Minimal human interaction (using ideas such as a highly adaptive network topology and properties of self-organization and self-maintenance to reduce the need for human interaction other than data processing).

2. Sensors Review

The following sections focus on the passive infrared and magnetic sensors as they are used in the experiments.

a. Magnetic Sensor (MS)

Magnetic sensors measure magnetic flux or the strength and direction of a magnetic field; a variation in the magnetic field is caused by an input which creates or alters the magnetic field such as a ferrous object moving within the earth's magnetic field (see Figure 12). The technology for sensing magnetic fields has evolved tremendously due to stringent demands for improved sensitivity, smaller size, and compatibility with electronic networks. Various sensing technologies are used [24] which include magnetoresistive devices (measuring electrical resistance as a function of the applied or ambient magnetic flux) and coil or flux-gate sensors (measuring differences in the magnetic field at the ends of a vertical rod).

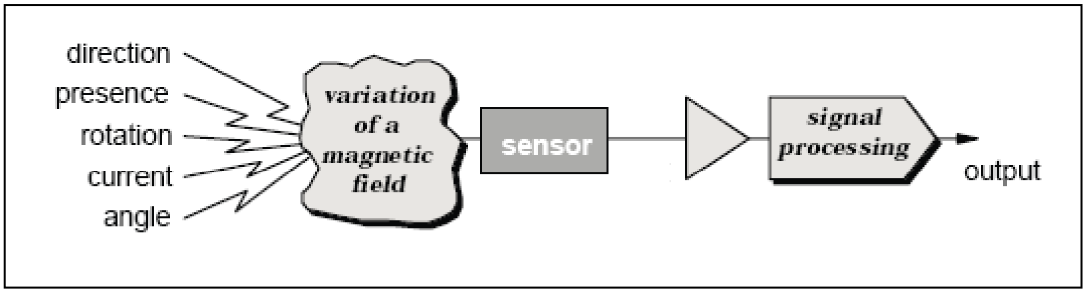


Figure 12. Schematic of magnetic sensing (from Ref. [24]).

b. Passive Infrared Sensor (PIRS)

The term “passive” means there is no emission of energy by the sensor; it merely receives incoming infrared radiation (black body radiation). In general, a passive infrared sensor is an electronic device that measures total infrared light radiating from objects in its field of view. They detect motion due to a difference in temperatures, as when a human enters its field of observation with the background at another temperature. Passive infrared sensors are commonly used in burglar alarms and motion-activated light systems.

c. Other Sensors

Due to the nature of IEDs and their emplacement techniques, a number of other sensors such as seismic, acoustic, radiation, and chemical sensors may be suitable for an IED detection scheme.

Common seismic sensors detect and measure the Earth’s ground motion, i.e. vibrations. These vibrations are similar to sound waves in air, but span a wider frequency range that extends well below the threshold for human hearing – which could serve as part of an intrusion detection system to detect potential IED emplacers at unfrequented places. It may also potentially be used to detect vehicular IEDs by perhaps characterizing anomalous vehicular movements.

Acoustic sensors are already used extensively in a number of military applications, particularly for the benefit of acquiring threat information at stand-off distances. Such sensors usually contain a piezoelectric element which can be configured to detect various audio signatures. Similar to seismic sensors, acoustic sensors could be used to detect anomaly signatures as part of an intrusion detection system.

Radiation sensors span a wide range of functionality depending on their usage, i.e., types of radiation. In the instance of an IED detection system, an electromagnetic radiation sensor may be useful to detect foreign electromagnetic signatures of wireless devices used in remotely-activated IEDs, i.e. mobile devices, remote controllers, etc.

Chemical sensors are perhaps one of the most widely researched sensors in current IED detection systems. Due to the nature of explosives, chemical sensors are particularly useful in detecting the nitrate constituents which are common to most IEDs.

3. Introduction to Crossbow Technology

Crossbow Technology Inc. is a solution supplier for wireless sensor networks and inertial sensor systems (refer to www.xbow.com for the company profile and its MSP410 User Manual). The sensor system that is used in this research is the MSP410, which comprises of 8 sensor nodes (termed "motes") along with a "base station" (see Figure 13). A good overview of MSP410 and other Crossbow's sensor systems is provided in [25, 37].

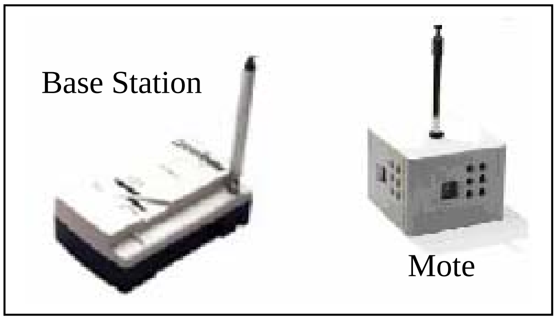


Figure 13. Crossbow MSP410 Base Station and Mote (from Ref. [25]).

The deployment layouts recommended by Crossbow for typical security applications are depicted in the following figures.

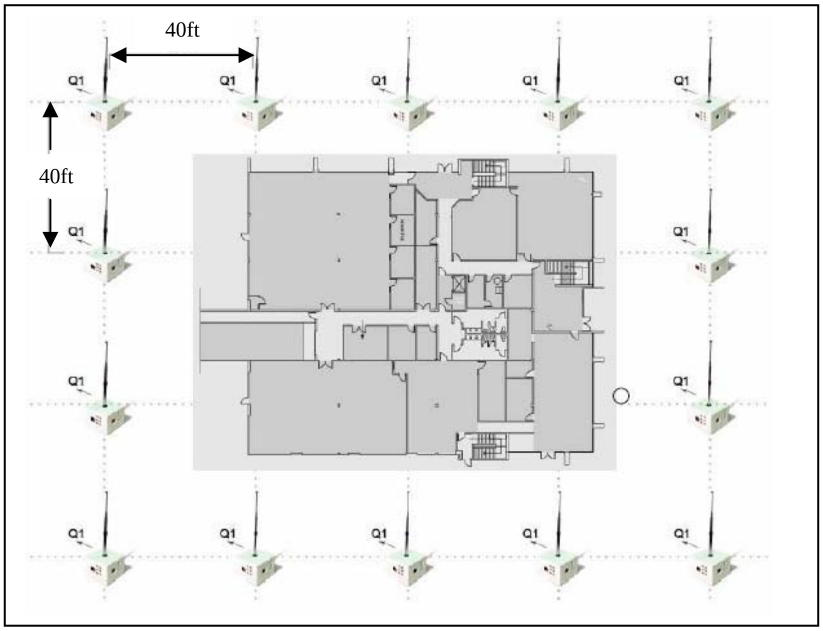


Figure 14. Perimeter-monitoring deployment (from Ref. [25]).

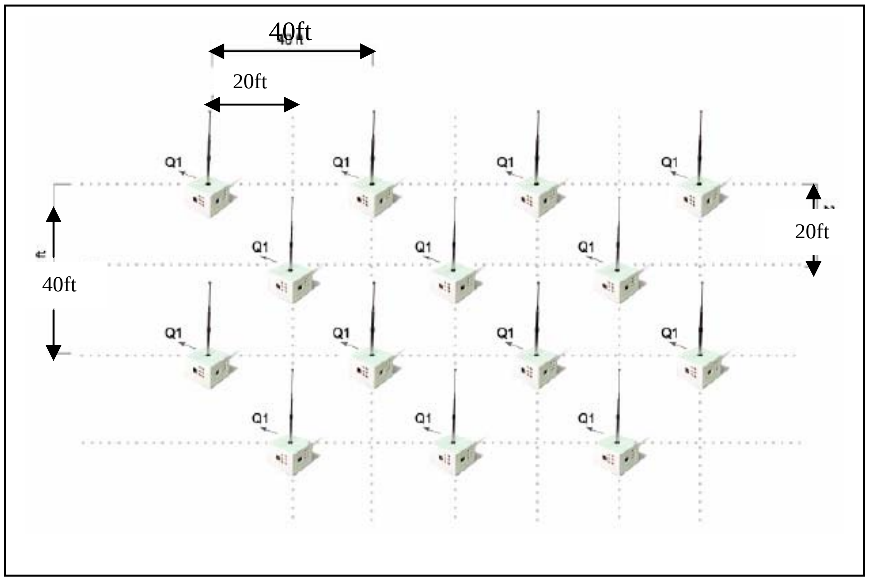
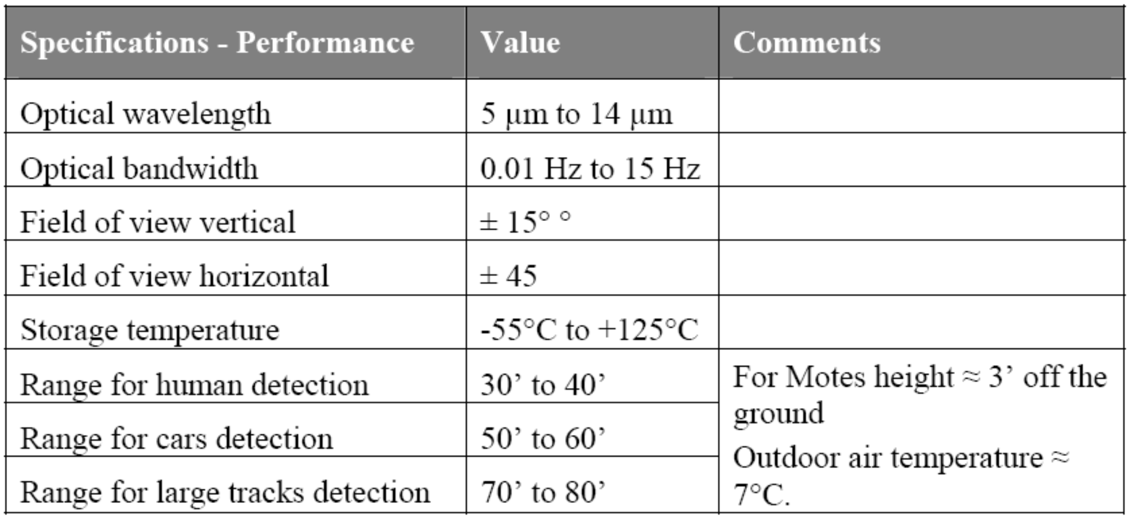


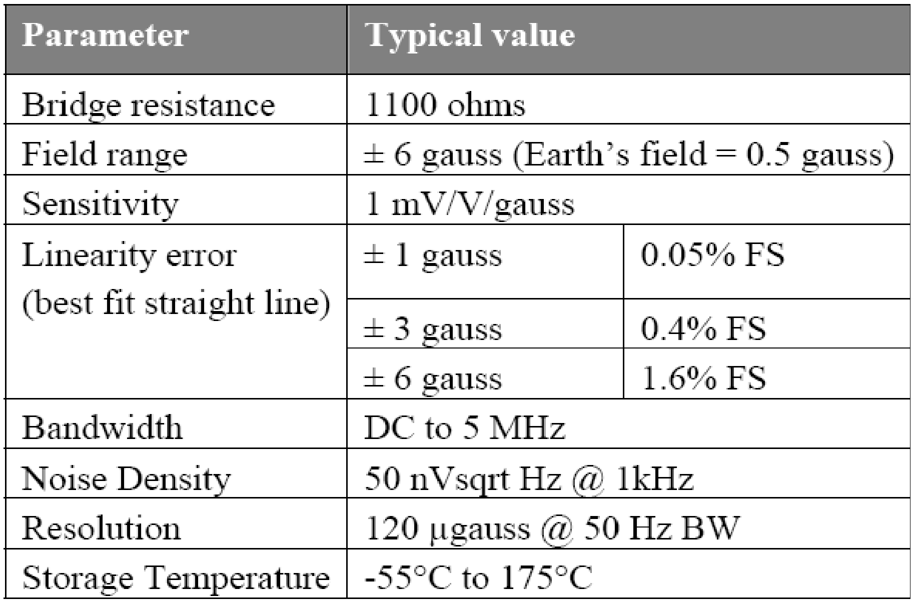
Figure 15. Dense-grid monitoring deployment (from Ref. [25])

Each mote contains a set of magnetic and infrared sensors. The infrared sensor can provide coverage of 360 degrees; the magnetic sensor is a two-axis magnetic field disorder detector. The following tables give the specifications of the sensors.



Specifications - Performance	Value	Comments
Optical wavelength	5 µm to 14 µm	
Optical bandwidth	0.01 Hz to 15 Hz	
Field of view vertical	± 15° °	
Field of view horizontal	± 45	
Storage temperature	-55°C to +125°C	
Range for human detection	30' to 40'	For Motes height ≈ 3' off the ground Outdoor air temperature ≈ 7°C.
Range for cars detection	50' to 60'	
Range for large tracks detection	70' to 80'	

Table 3. Specifications of MSP410CA Mote PIR sensor (from Ref. [25]).



Parameter	Typical value	
Bridge resistance	1100 ohms	
Field range	± 6 gauss (Earth's field = 0.5 gauss)	
Sensitivity	1 mV/V/gauss	
Linearity error (best fit straight line)	± 1 gauss	0.05% FS
	± 3 gauss	0.4% FS
	± 6 gauss	1.6% FS
Bandwidth	DC to 5 MHz	
Noise Density	50 nVsqrt Hz @ 1kHz	
Resolution	120 µgauss @ 50 Hz BW	
Storage Temperature	-55°C to 175°C	

Table 4. Specification of MSP410CA Mote magnetic sensor (from Ref. [25]).

III. EXPERIMENTATION METHODOLOGY

A. TEST ENVIRONMENTS

Two sets of test environments are distinguished here. The first set of test environments was the quadrangle outside a public mall and an actual public street, which were used to establish background thresholds (see Test Case A). The other set of test environments were simulated in the school compound for the conduct of Test Case B, C and D (see Figure 16 and 17) so that they contained as many signatures as possible that occur in actual environments, albeit with limitations on the number of human and vehicular actors. For instance, a controlled number of human and vehicular actors were introduced into the simulated environments to simulate infrared signatures and magnetic signatures of large ferrous objects such as post boxes, escalators, trash bins, and lamp posts; a circuit board with batteries to simulate IED circuitry, and wireless devices such as cell phones and remote-control toys to simulate wireless electromagnetic signals.

1. Shopping Malls

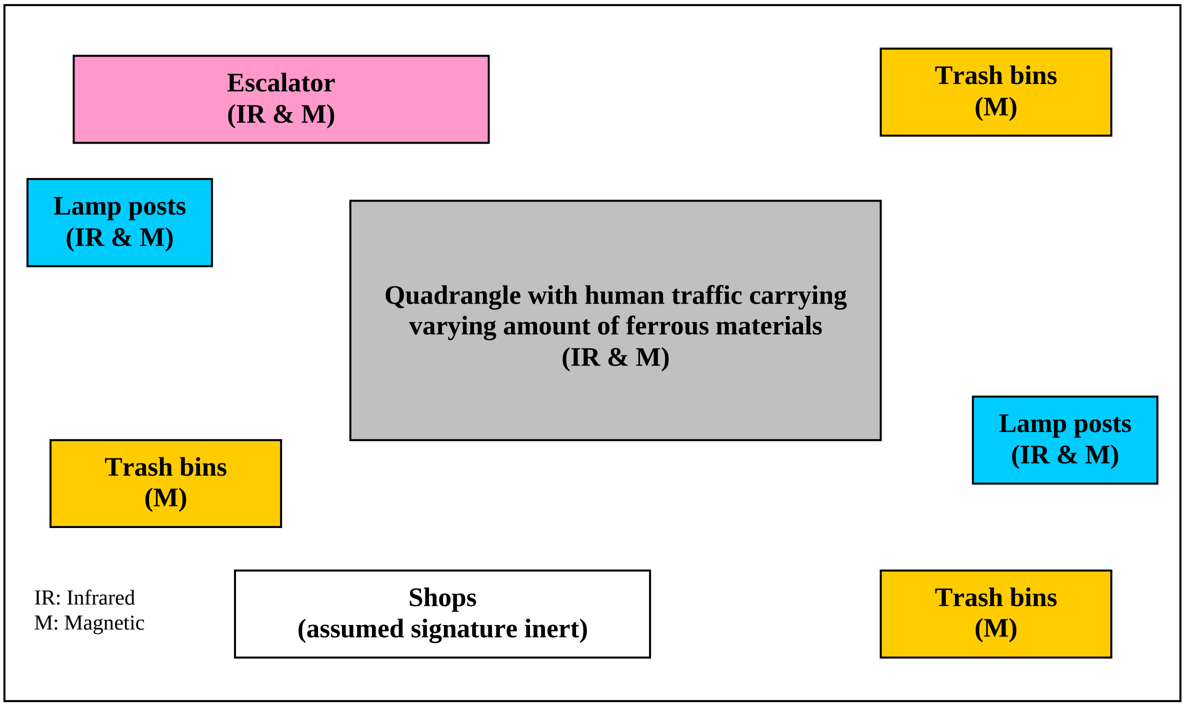


Figure 16. Layout of a simulated shopping-mall test environment.

It is difficult to conduct experiments in a real shopping mall for reasons of authorized accessibility. Figure 16 shows our simulated mall design including such representative objects as lamp posts, escalators, and trash bins. The idea was to include a controlled amount of signatures while experimenting with a suitable placement of sensors to detect foreign signatures.

2. Roadsides/Streets

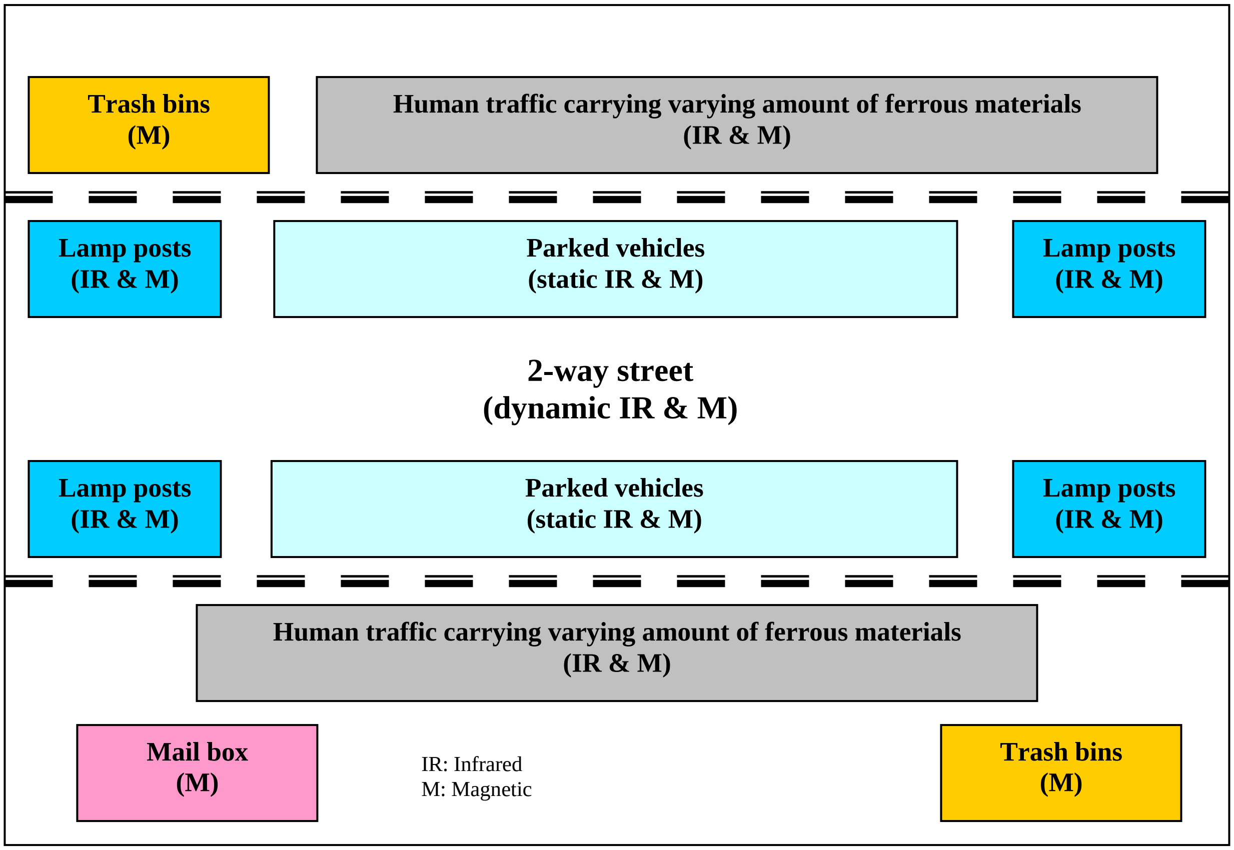


Figure 17. Layout of a simulated roadside/street test environment.

Figure 17 shows our layout for a simulated roadside / street environment. This is readily available unlike a shopping mall, albeit with a certain randomness of signatures introduced by passing vehicles.

3. Establishment of Thresholds

We used Crossbow sensors to capture background data or clutter (in actual environments) to be used in the simulated test environments. These data are processed and thresholds established for normal infrared and magnetic signature readings. These were used to determine when foreign entities with abnormal signatures entered the test environments. It must be emphasized that these threshold values may not necessarily hold true for all environments.

4. Test Cases

Test cases were limited due to resource constraints. Every effort, however, is made to ensure meaningful results are derived from these test cases to support or refute our proof-of-concept in the feasibility of using wireless sensor network for IED detection. The independent variables in these tests were:

- N : number of sensors
- X : number of iron nails
- H : height of sensor node relative to ground level
- d : distance from Crossbow sensors
- t : thickness of trash bins or similar containers / mediums

a. Test Case A – Determination of background thresholds

Test Case A was conducted at a quadrangle outside a mall and along a one-way street for test environment A and B respectively during both peak (1200-1400) and off-peak (1600-1800) periods. The sensor motes were interspersed at appropriate distances (not necessarily conforming to the settings as recommended by Crossbow) due to physical constraints.

b. Test Case B – Study of X

We examined the number of nails (or amount of ferrous content) and distance *d* which were required to trigger the Crossbow magnetic sensors. Nails permitted ease of quantification, i.e., *X* nails required to trigger a magnetic reading. With the relationship between *X* and *d* determined, Test Case B experimented with a single actor carrying *X* nails into the simulated test environment. The purpose of this test was to examine the robustness of the sensors to detect and report foreign infrared and magnetic signatures. It used an alert dialogue box, as well as presenting the general locations of the signatures. The experiment also attempted to determine a feasible topology of sensors for effective detection.

c. Test Case C – Study of IED circuitry

The main ferrous component of IEDs that are commonly emplaced in postal or trash receptacles are usually electrical circuit boards, as compared to an IED composed of, say, an artillery round whereby the casing is large and usually ferrous and hence producing a larger magnetic signature. Test Case C experimented with an electrical circuit to simulate an IED circuitry as shown in Figure 18 to determine the threshold of a typical electrical circuit that could be used for wireless activation of IEDs.

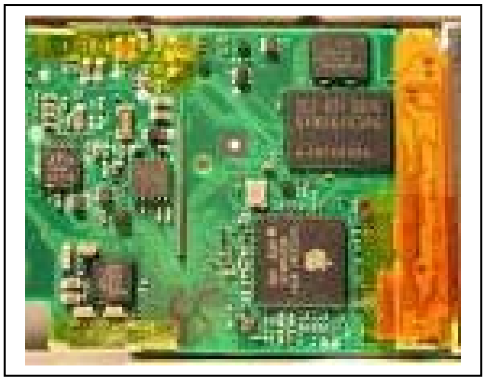
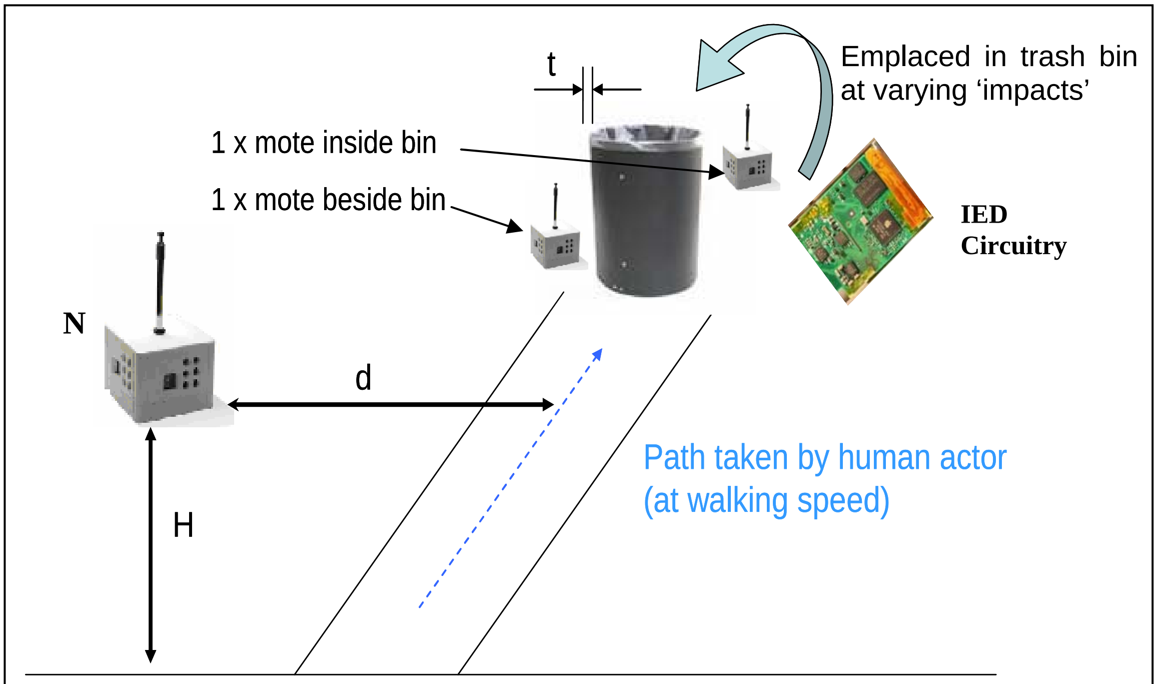


Figure 18. Depiction of a typical electrical circuit.

d. Test Case D – Study of Trash Receptacles

Trash receptacles were common to both test environments. Test Case D exploited the results obtained from prior tests. Experiments were conducted with a single actor carrying the IED circuitry into the simulated test environment and approaching a trash receptacle along a fixed path as depicted in Figure 19. The purpose of this test was to examine the robustness of the sensors in detecting and reporting foreign magnetic signatures. Further tests investigated the effects of the thickness of the trash receptacle and the waste items (comprising primarily of beverage cans) on the sensitivity of the Crossbow sensors. It is hoped to isolate this particular source of threat by finding magnetic signatures of potential IEDs. Test Case D also examined the efficiency and effectiveness of sensor detection with human actors carrying IED circuitry.


t
Emplaced in trash bin at varying 'impacts'
1 x mote inside bin
1 x mote beside bin
IED Circuitry
N
d
H
Path taken by human actor (at walking speed)

N: 8 of these motes are interspersed in the two test environments; not always adhering to the recommended spatial requirements due to physical constraints

Figure 19. Depiction of test case D.

B. DETECTION IMPLEMENTATION

This section explains the approach to detecting ferrous metals, IED circuits, and unexploded ordnance using the MSP410 Crossbow platform and its software to gather data from the sensor network. The process was (illustrated in Figure 23):

- Gathering of raw data from Crossbow motes upon detection of foreign infrared and/or magnetic signatures;
- Identifying and extracting the relevant packets from the data to determine their value in measurable units;
- Comparing of captured readings with thresholds through a database server established previously;
- Issuing a signal or alert to the user platform upon positive identification.

1. Software

The software for accessing and managing data captured by Crossbow motes included MoteView, SerialForwarder, and TinyOS (the operating system).

a. MoteView

MoteView is a simple user control of the Crossbow sensor system setup, which comes as a software package with a development kit. It works on a three-layer architecture using a mote layer, a server layer, and a client layer (see Figure 20); the MoteView software exists on client machines in the client layer. Depending on the program which is used in the Crossbow motes (usually compiled in TinyOS environment), the data is captured in accordance to the programmed tasks and is stored or logged in the databases in the server layer. From here, the user can retrieve selected data on the MoteView screen. There are options to view the data logged in the server layer as raw data, measurement data (raw data converted to appropriate units of measure), charts, or in a spectrum view.

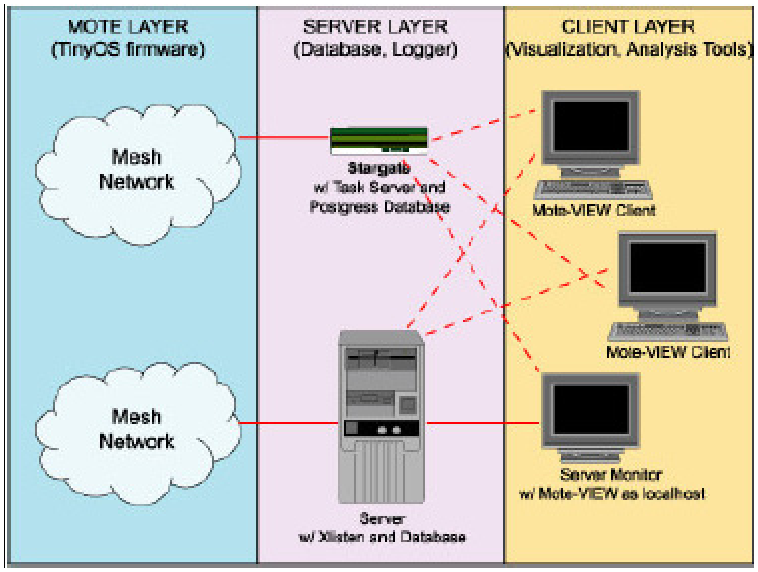


Figure 20. Depiction of data flow within MSP410 three-layer architecture.

b. Surge-View and SerialForwarder

Surge-View is a set of software tools provided by Crossbow which contains the Surge Graphical User Interface, the Stats, and the HistoryViewer programs. Through the Surge-View, the user can see the sensors' board data to aid in studying the system's networking issues.

SerialForwarder is a Java program used to read packet data from a computer's serial port, and forward it over a server port connection, so that other programs can communicate with the sensor network via a sensor network gateway. SerialForwarder updates the packet counters in the lower-right hand corner of the interface window and does not display the packets itself. SerialForwarder listens for network client connections on a given TCP port, and forwards TinyOS messages from the serial port to the network client connection and vice versa. Many TinyOS applications run with the support of the SerialForwarder program upon startup such as Listen.class which will be covered later.

c. TinyOS

TinyOS is an open-source operating system that runs embedded in sensor nodes and is used in many wireless sensor networks. It contains built-in interfaces, software components, and configurations that programmers can use to build their applications in a modular structure. Some of these components read data from and send data to sensor nodes, organizing broadcasting methods to all sensors, and interpret data. One of the components Listen.class is used to read sensor data upon a trigger of events from the mote that senses, and this component is vital for first-hand information and tracking of objects. As the motes would report on all foreign signatures within its sensitivity range, modifications had to be made to the Listen.class whereby only those signatures exceeding a particular threshold would be reported. Thereafter the motes would resume to 'idle' mode. Typically the motes are able to distinguish and report two signatures occurring separately in the order of milliseconds as independent events as indicated by the timestamps (with an unique sample number attached to each event), i.e. 12:30:10 for sample #200 and 12:30:10 for sample #201.

2. Packet Description

To read packets for magnetic and infrared values, the representation of data must be understood. The MSP410 motes uses the Active Message format or AM, which is encapsulated data from the sensor network forwarded to the base station. The format is presented in Figure 21 [37]. The UART Address, Type, Group ID, Sensorboard_ID and Packet_ID form the Headers and Networking Data. In addition, there is a 5 byte TOS Header at the start outside the AM structure. Upon executing a Java program called Listen.class that outputs raw data onto the screen, the breakdown of the data segment is noted as below, using references from the *Getting Started Guide*, Crossbow, 2005.

UART Address	Type	Group	Length	Sensorboard_ID	Packet_ID	Data	CRC

Figure 21. Depiction of Active Message (AM) data format.

1B	7B	1B	2B	1B	1B	2B	2B	2B	4B
Node ID	Unidentified	Parent ID	seq	vref	quad	pir	mag	audio	Unidentified

Figure 22. Breakdown of data segment in Active Message format.

Figure 22 above shows the breakdown of the "data" segment of the AM structure shown in Figure 21. The Node ID is represented as 1 byte and the next 7 bytes are unspecified. The audio bytes are always read as 0 in our implementation as the audio sensor was disabled in all of the motes used. Segment packets are read from the raw data and converted to decimal format for further use.

3. Flowchart of Listen.class and Modification

The Listen.class is a Java program that can read the packets from the motes of the sensor network via the base station and display the data in hexadecimal. It can open a serial port directly, read the raw sensor data, and display it. However, SerialForwarder makes it easier to run the Listen.class and display the data on the screen. And at the same time, other applications can read the same packets off SerialForwarder server port.

The flow of the Listen.class is illustrated in Figure 23. It identifies the mote that has been triggered by an event and captures its packet readings for analysis, using relevant data stored in a database, of whether they suggest particular types of IEDs. In our experiments, the Listen.class program was modified (see Appendix A).

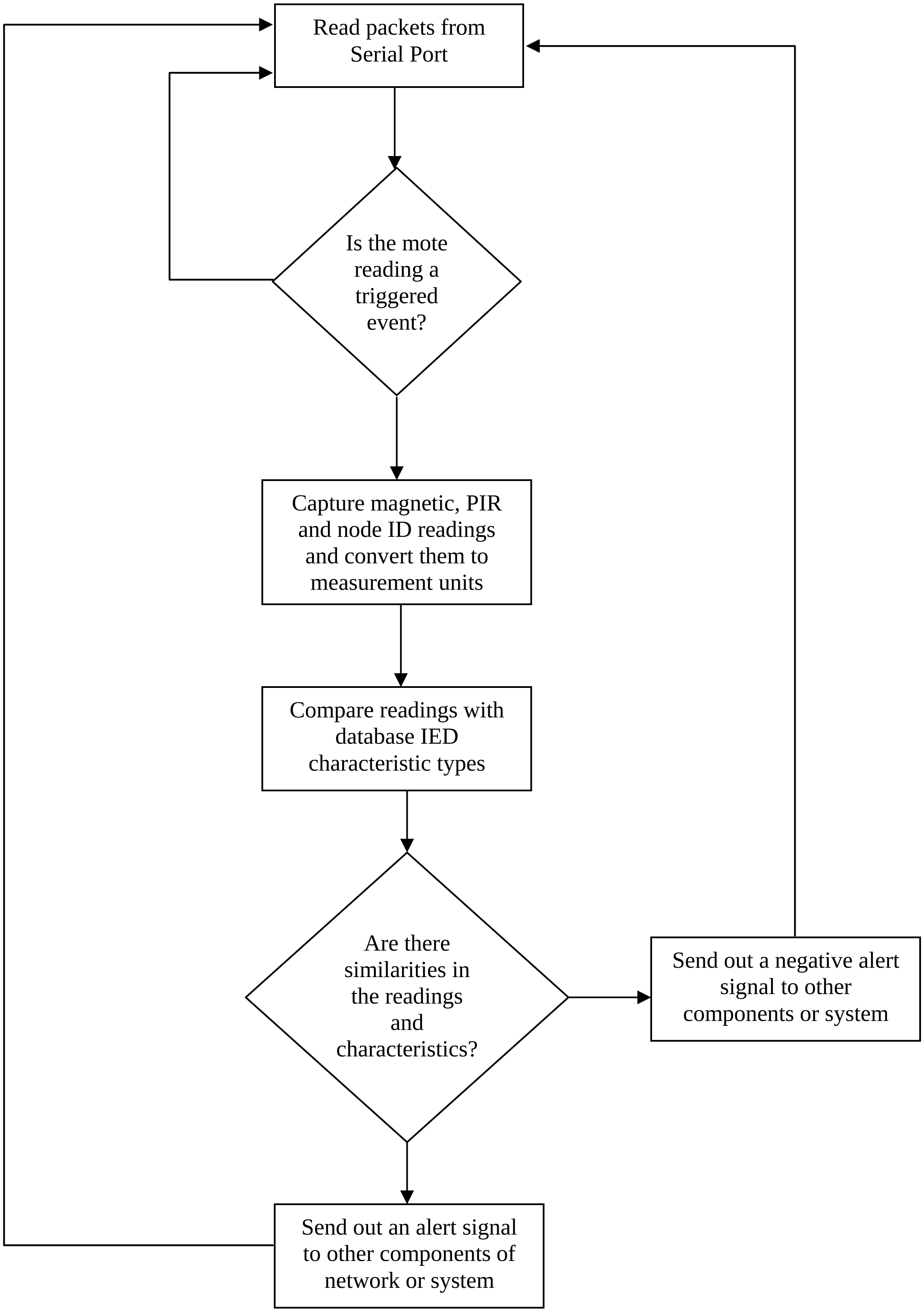

Read packets from Serial Port
Is the mote reading a triggered event?
Capture magnetic, PIR and node ID readings and convert them to measurement units
Compare readings with database IED characteristic types
Are there similarities in the readings and characteristics?
Send out a negative alert signal to other components or system
Send out an alert signal to other components of network or system

Figure 23. Modified flow of Listen.class.

IV. EXPERIMENTAL RESULTS

A. TEST CASE A – TEST ENVIRONMENT THRESHOLDS

Test Case A was conducted at a quadrangle near a shopping mall (Figure 24) to simulate a confined-space environment consisting primarily human actors and no vehicles. We were unable to conduct the experiment in the shopping mall itself due to reasons of practicality and lack of authorization. Human actors carried with them random amounts of ferrous materials such as laptops, metal accessories, mobile phones, providing limited but somewhat representative magnetic and infrared signatures.

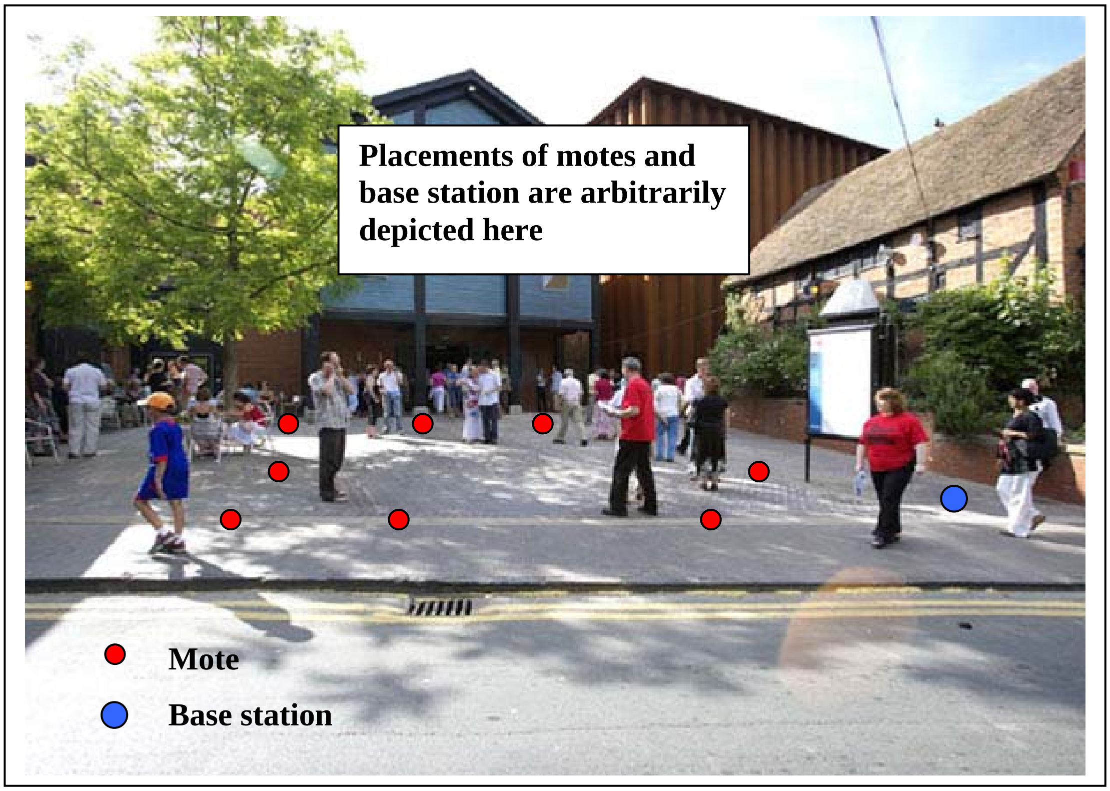

Placements of motes and base station are arbitrarily depicted here
● Mote
● Base station

Figure 24. Depiction of experimental setup for test environment A.

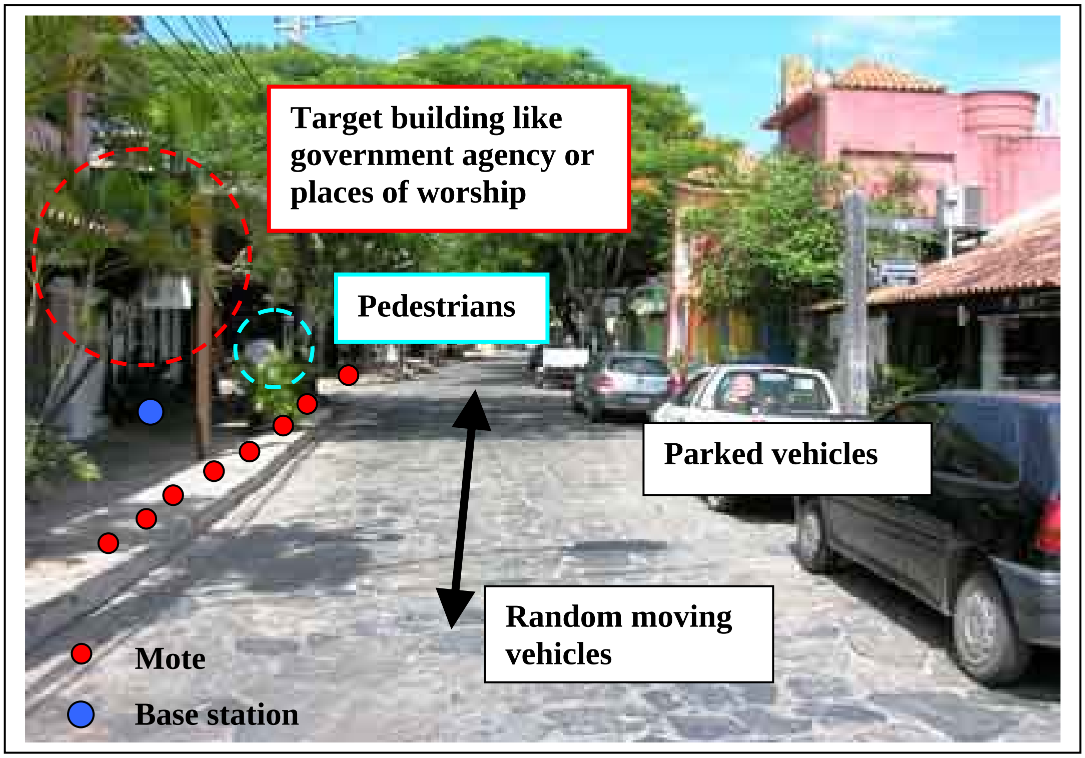


Figure 25. Depiction of experimental setup for test environment B.

Figure 25 above shows the street used in test environment B, which had both human actors and vehicles (both parked and moving). A target area was assumed and the motes were placed along the outer perimeter of the road. The test parameters for both environments were:

- *Time*: Peak period (1200-1400hrs)

  Off-peak period (1600-1800hrs)
- *Duration*: 2 x 30min per experimental run for both periods for 2days
- *Weather*: nil precipitation, cloudy
- *N*: 8
- *H*: 0cm relative to ground level

A summary of the results is presented in Table 5 (detailed data is not included for this test due to the massive number of readings). These values are averages of the registered readings.

Test Environment A		Test Environment B	
Peak period			
Magnetic	Infrared*	Magnetic	Infrared
1375	695 (-)	22147	420 (-)
Off-peak period			
520	987 (-)	21460	413 (-)

*Original infrared value for Crossbow sensor is at 1023units. The detection of presence of IR is represented by a decrease in the original infrared value hence the (-).

Table 5. Tabulation of thresholds for test environments A and B.

B. TEST CASE B – STUDY OF X

The experimental set-up is shown (overleaf) in Figure 26. The height of the mote was tested at heights of 0 cm, 45 cm, and 80 cm, representing ground-level, knee, and chest height respectively. The latter two are the heights at which a person would normally be carrying an object.

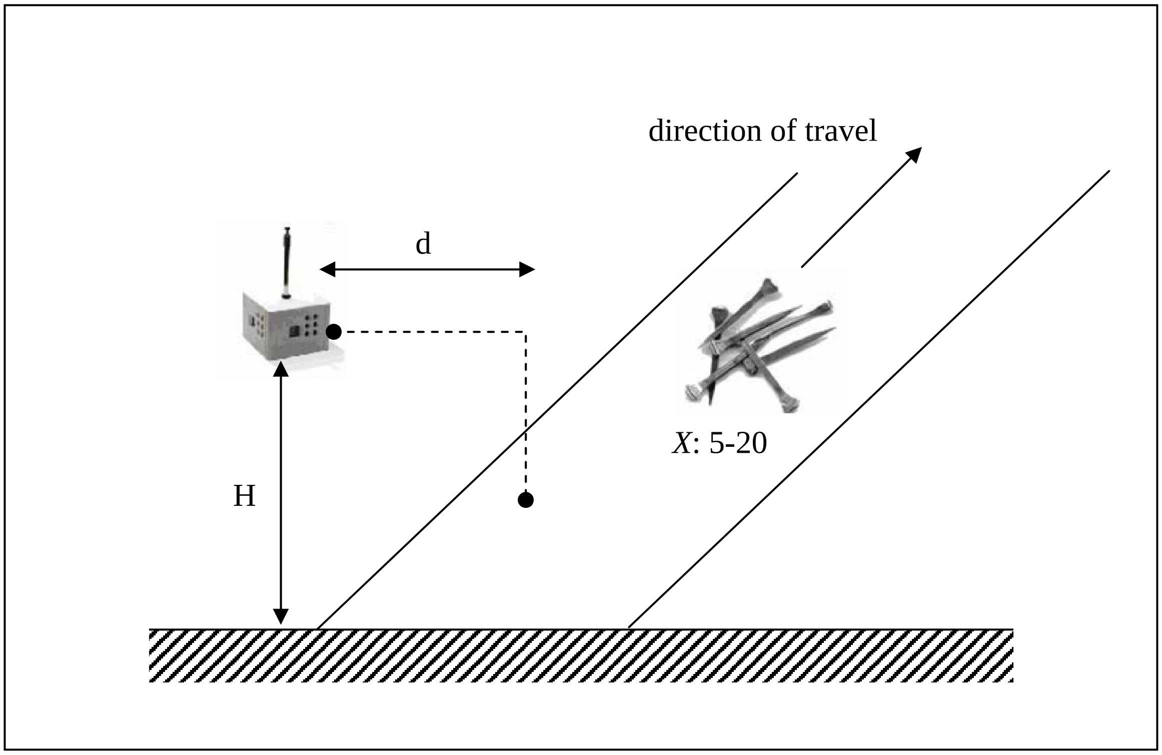


Figure 26. Experimental setup for test case B.

The test parameters were:

- *Repetitions*: 20 runs
- *X*: 5, 10, 20
- *H*: 0cm, 45cm, 80cm
- *d*: 10cm, 50cm
- *traveling speed*: walking pace

A summary of the results (magnetic readings only) is presented in Table 6 (see Appendix B for detailed data). These values are an average of the registered readings.

X / nails	Magnetic readings at H / cm					
	0		45		80	
	Distance from mote, d / cm					
	10	50	10	50	10	50
5	207	144	559	560	488	492
10	215	150	667	596	654	512
20	219	184	882	598	886	534

Table 6. Tabulation of magnetic readings for test case B.

C. TEST CASE C – STUDY OF IED CIRCUITRY

The experimental setup for Test Case C was similar to B, except that the nails were now replaced with an IED circuitry. A summary of the results (magnetic readings only) is presented in the following table (see Appendix C for detailed data). These values are an average of the readings.

H / cm d / cm	Magnetic Readings		
	0	45	80
10	294	589	680
50	221	578	619

Table 7. Tabulation of magnetic readings for test case C.

D. TEST CASE D – STUDY OF TRASH RECEPTACLES

Test Case D is of interest considering the vulnerabilities associated with trash receptacles; they are common to all types of environments, are publicly accessible, and so provide convenience for emplacement of IEDs. Trash bins not only conceal the explosive device, but can maximize the intensity of the explosion by spraying shrapnel at great distances. The U.S. Department of Homeland Security has published an "Approved Product List for Homeland Security" [8, 35] which outlines the use of "blast resistant trash receptacles" to contain the explosive effects resulting from an IED detonation.

Two motes were used in our experiment: one in the trash bin and one beside it. The bin was filled with common household trash (such as rubber, textiles, leather, plastics, metals, glass, paper and food scraps) with a human actor walking toward it and dropping the circuitry depicted in Figure 19. A report in 2005 [36] said that beverage cans are the most common metal wastes generated; this prompted experiments with drink cans as well. It is reported in [33] that most drink cans in the U.S. are made of aluminum (which is a non-ferrous material) which is undetectable by magnetic sensors (this was verified using Crossbow sensors). The purpose of our experiment was to isolate and attribute magnetic triggers to potential IED circuitry.

Two other experiments were conducted to investigate the effects of the receptacles' thickness and the effects of the emplacement force at which an IED was emplaced had on the sensitivity of the magnetic sensors (with no change to the size of circuitry). Results from latter could be useful for further study of anomalous behavior of people loitering [30] around trash bins.

Thicknesses of typical trash receptacles range from 0.2 cm to no more than 1 cm for most settings such as in shopping malls, airports, hospitals, and other communal areas. Experiments were conducted for t = 0.2 cm, 0.5 cm and 1 cm, and H = 0 cm, 45 cm and 90 cm. The height of the trash was assumed to be 1/3 the height of the trash bin. Common household plastic cardboards were wrapped around the main housing of the trash receptacle to increase t. It was infeasible for these experiments to use identical material as that of the plastic trash receptacle.

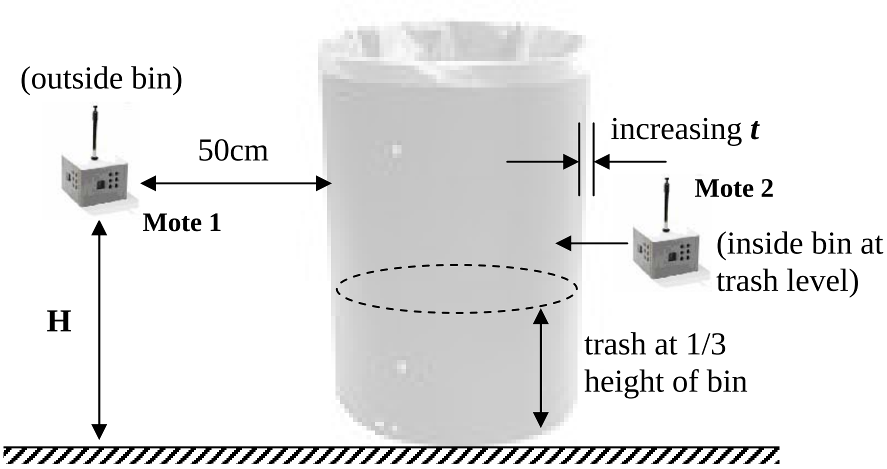


Figure 27. Detailed experimental setup for test case D.

H / cm t / cm	Mote 1			Mote 2		
	0	**45**	**90**	**0**	**45**	**90**
0.2	0	483	497	509	516	539
0.5	0	285	455	-	-	-
1	0	268	421	-	-	-

Table 8. Tabulation of magnetic readings for test case D (variation with t).

The force that one uses to deposit trash may be a useful indicator of IED emplacement [21]), detectable by the changes in magnetic readings of Crossbow magnetic sensors. Two cases were investigated, gradual versus sudden emplacement for t = 0.2cm and H = 90cm. ("Gradual" is defined here as a gradual movement of IED into the mouth of the trash receptacle and placing it just above the trash whereas "sudden" is defined as dropping the IED from the mouth of the trash receptacle.) A summary of the results (magnetic readings only) is presented in the following table (see Appendix D for detailed data). These values are an average of the readings.

Mode H/cm	Gradual	Sudden
90	539	819

Table 9. Tabulation of magnetic readings for test case D (variation with emplacement force).

V. FINDINGS AND ANALYSES

A. TEST CASE A

For test environment A, Figure 28 shows that the motes could effectively sense the presence of human agents (or other infrared emissions) in the environment with frequent triggers throughout the 30-minute period, and an observable difference between the peak and off-peak period. Magnetic triggers, on the other hand, were infrequent and sporadic as indicated by the spikes (some agents were carrying laptops), which suggests that few agents carry ferrous materials. The infrequent magnetic triggers could also be attributed to the sensitivity range of the sensor motes, either due to a low ferrous content carried by each agent or that the agents were not within the sensitivity range. Some inefficient coverage of the test environment resulted from spatial constraints in the quadrangle, as well as the limited number of motes (8) that we had for the experiment. The low frequency of magnetic readings also suggests establishing a magnetic threshold using the mean value would not be accurate.

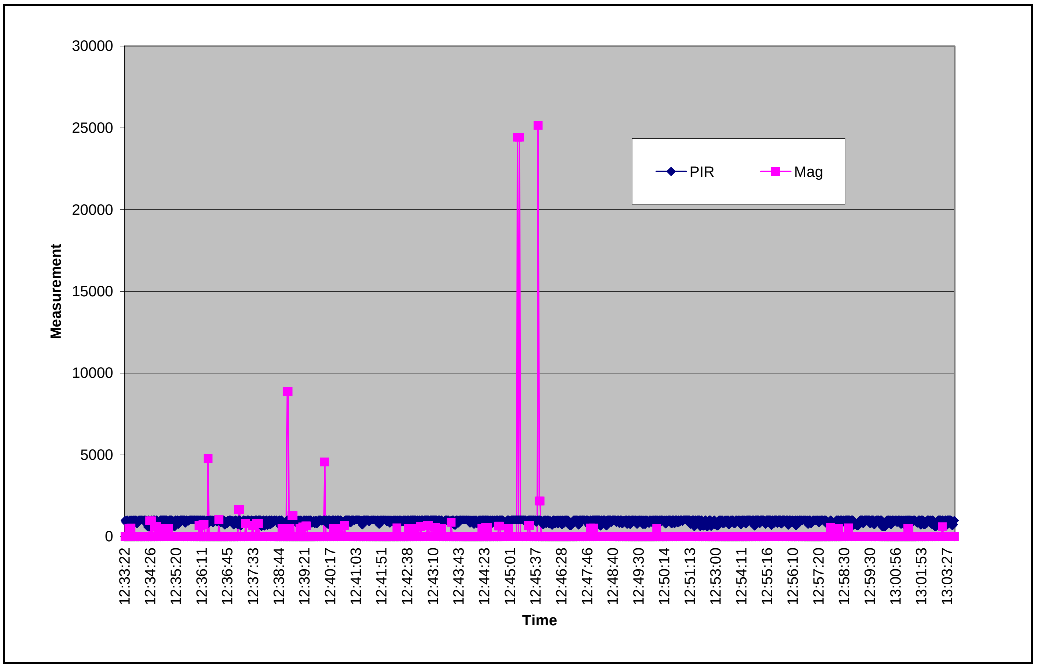


Figure 28. Graphical plot for passive infrared and magnetic readings registered during peak period in test environment A.

In test environment B, with vehicular movements unlike environment A, there were frequent magnetic triggers with corresponding passive infrared detections (i.e. heat from engines). However, there were positive magnetic triggers without any change in passive infrared (for the base level of 1023 units) as highlighted in Figure 29. This could reflect a cold vehicle engine just turned on. Environmental factors such as air disturbances or fluctuations in ambient temperatures were possible influences as well [34]. (Electromagnetic interference should not be a problem with Crossbow sensors as its magnetometers have a bandwidth of 400 Hz or less, so even strong radio-frequency sources like cell phones and base stations should not affect magnetic readings.) Another possible cause could be the limited field of view of the motes so that a single vehicle would be perceived as separate objects, a heated engine and a cold body. The large average magnetic reading of 950 units suggests that magnetic sensors alone in such an environment may not detect PIEDs which contain a low ferrous content.

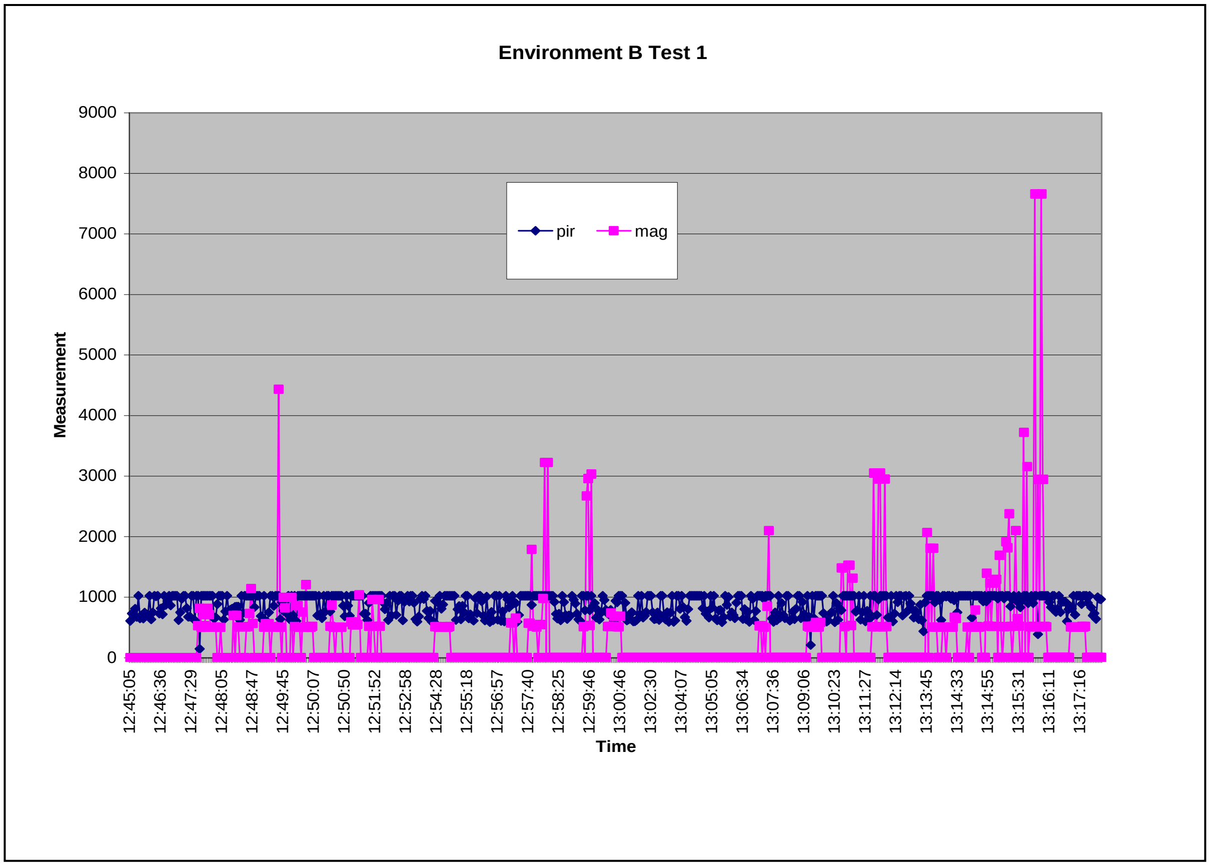


Figure 29. Graphical plot for passive infrared and magnetic readings registered during peak period in test environment B.

B. TEST CASE B

Infrared values were not used in Test Case B since the aim was to check if the magnetic sensors were robust enough to detect foreign magnetic signatures. For gathering of data the Mote-View software was used. Looking at the variation in the distance parameter d, there is a higher magnetic reading for nails closer to the motes than further away. For instance, at H = 0 cm height or ground level, the average reading for 5 nails was higher for d = 10 cm than for d = 50 cm. This observation highlighted the need for a good topology of the sensor deployment and sufficient quantity of sensors. There were fewer false positives for H = 45 cm and 80 cm than for H = 0 cm or ground level. This could be attributed to the sensors’ two-axis magnetometer circuit boards (which are aligned horizontally when placed flat on a surface) which had a greater sensitivity for objects aligned with the motes. The low false negative rate for H = 45 cm and 80 cm is encouraging as these are the heights that agents are expected to carry IEDs (either in bags slung over their shoulders or in their hands at about waist level). Hence emplacing the motes at a sufficient height is important for sensor deployments.

As mentioned in Chapter II, Crossbow MSP410 system recommended deployment configurations were dense grids and perimeter grids. Our experiments were conducted using the dense-grid deployment with the motes positioned at an interval of 5 ft (the recommended spatial interval is 40 ft). Two deployment directions of the motes were tried as shown in Figure 30 and 31. The deployment shown in Figure 31 was more sensitive (with magnetic readings exceeding 1000 units) than that of Figure 30. This could be due to the magnetic sensor axis (located along the sides of each mote) having a greater area of exposure to signals from the passageway.

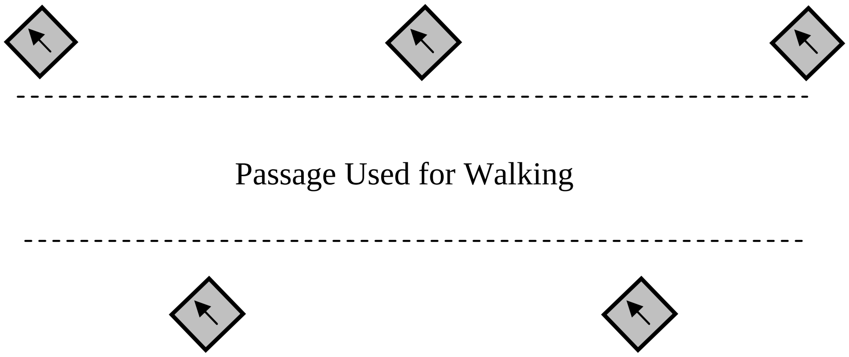


Figure 30. Directional placements of motes at an angle to the passage.

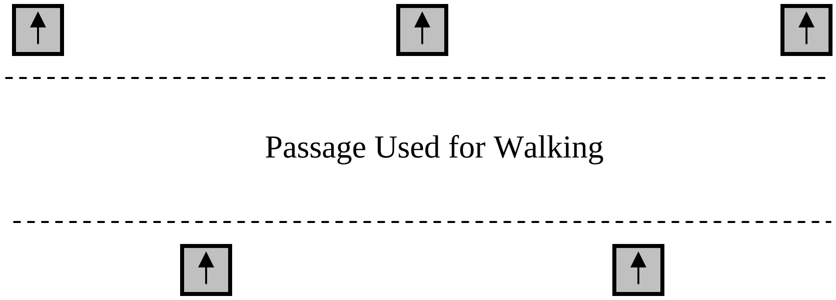


Figure 31. Directional placements of motes perpendicular to the passage.

C. TEST CASE C

Test Case C was conducted in similar fashion as was Test Case B except for the replacement of nails with the IED circuitry. Similar findings occurred. In particular, similar average magnetic readings were observed for both IED circuitry and nails though they were dissimilar in forms and sizes. This suggests that threshold-categorization of IED circuitry may not be possible using magnetic sensors alone as many other objects many trigger readings within the threshold range. Other characteristics such as chemical vapors would need to be incorporated to the detection scheme, and would require use of other sensors.

D. TEST CASE D

Some of the sensors could detect the human actor carrying the IED circuitry (with the showing of a dialogue box alerting of potential IEDs) as he approached the trash bin, but there were occasional false negatives by some motes attributable to the fact that the actor was out-of-range.

The two motes at the bin were largely successful in detecting the IED as it was dropped in the bin. The mote inside the bin had a 100% positive detection. The mote outside the bin registered lower magnetic readings and displayed similar trends as Test Case C, i.e. a number of false negatives for H = 0 cm, and 100% positive detection for H = 45 cm and 90 cm. The magnetic readings had several spike outliers possibly attributable to the disturbance of the mote as the IED was dropped, as both a movement of the mote or the presence of ferrous materials would trigger a change in magnetic flux.

The results for various bin thicknesses suggested an inverse relationship between a bin’s thickness and the strength of magnetic readings. Consequently, the mote outside the bin for t = 1 cm had a higher frequency of false negatives. The simulation of emplacement force, though crude, produced observable difference in magnetic readings. On average, the readings for sudden emplacement were about 30-50% higher than gradual emplacement (see Figure 32 and 33), which could be attributed to a higher rate of flux-cutting.

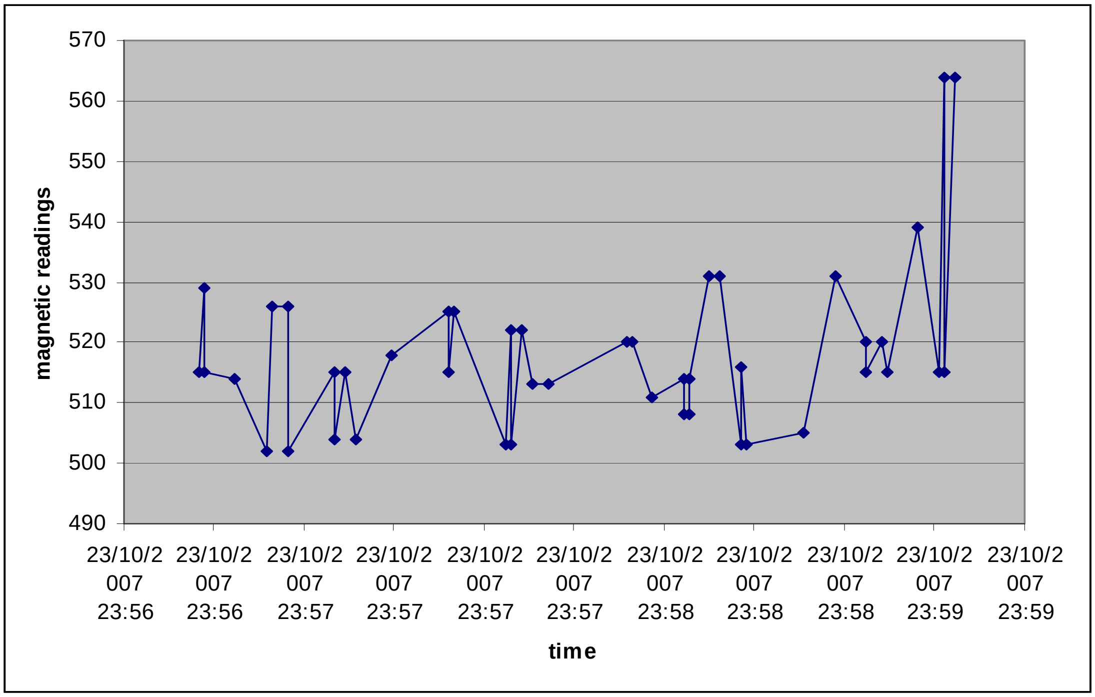


Figure 32. Graphical plot for magnetic readings for Gradual Emplacement for H = 90cm.

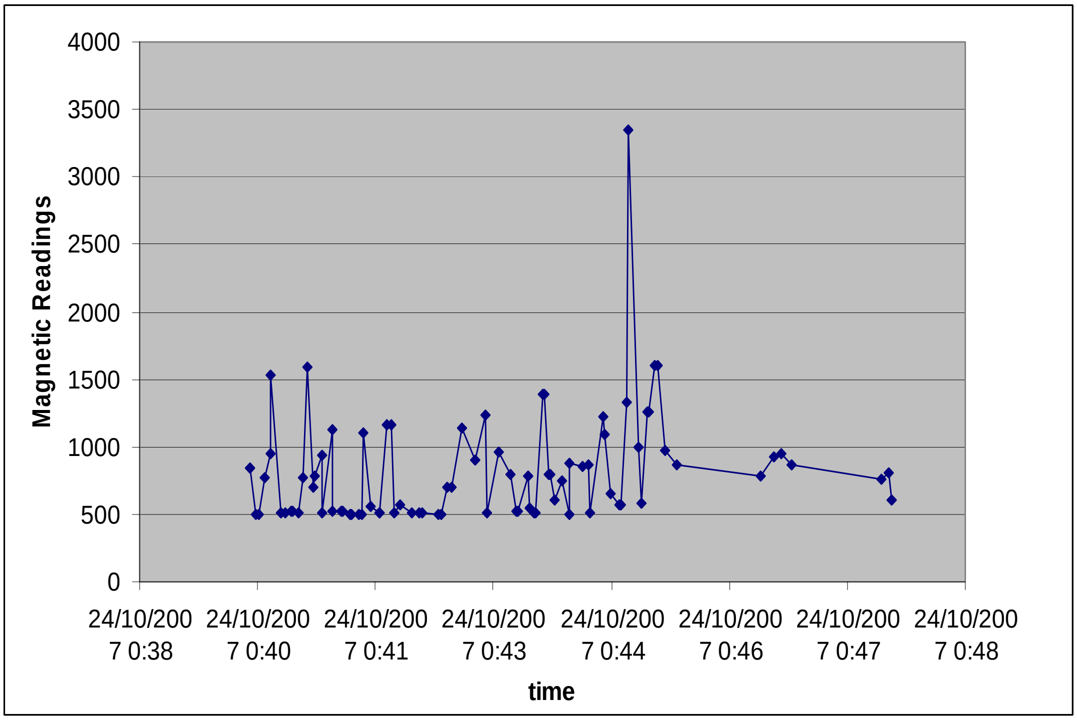


Figure 33. Graphical plot for magnetic readings for Sudden Emplacement

E. SUMMARY OF FINDINGS

- Crossbow sensors may not be suitable for characterization of small objects. Even for larger objects there must be other forms of sensing that will describe the granularity of materials so that there is a distinct contrast among their characteristics. This is vital in detecting possible IEDs and identifying them without raising high probabilities of false positives.

- The thresholds established in our experiments were averages of the readings; such computation is crude. The magnetic sensors could detect nearby metals, but were unable to differentiate an IED-type object. Hence, a more refined and multi-faceted algorithm needs to be developed to recognize a wider range of characteristics of an IED.

- Infrared sensors are good at detecting human traffic but are not particularly helpful for IED detection. Close proximity of ordinary objects was not detectable by infrared sensors as the sensing beams were used over a narrow angle. Moreover, there is no distinct radiation of IED objects which the sensors could capture. These sensors best serve as effective motion detectors when sited in rarely-frequented areas of the environment and deployed for perimeter surveillance.

- The sensors were highly susceptible to external influences such as air disturbances. In particular, magnetic readings were triggered even in the absence of ferrous materials. Infrared sensors are also unreliable in environments with temperature variations as well as wind changes.

- Magnetic sensors in isolation may not be suitable for IED detection since there are numerous ferrous or magnetic sources, especially in a mall environment. However when placed in specific receptacles such as postal or trash bins, magnetic sensors may help detect dubious trash.

- A limitation in the experiments was the number of sensor motes and the spatial constraints in their positioning, whereby there were a number of false positives. This is in part due to a lack of sensitivity of the magnetic sensors which suggests that many are needed for effective coverage.

- The topology of the sensors shown in Figure 31 could be a useful deployment template for threat scenarios where there are limited ingresses and egresses.

- Available power is a constant limitation in any outdoor deployment of wireless sensor networks. Our experiments required high levels of power consumption because the motes reported data frequently – each mote uses two 1.5-volt alkaline AA batteries and the mote’s lifespan is estimated at 250 hours and 12000 hours for constant active mode and sleep mode respectively (based on the estimated power consumption rates reported in [31] and [32]). Though there are algorithms to allow sensors to adapt when one or more motes are not functioning, the issue of power supply must be carefully addressed (i.e. simulation of power consumption) prior to deployment.

VI. CONCLUSION

A. SUMMARY OF RESEARCH

The research is focused on wide-area surveillance of communal environments for potential IEDs using wireless sensor networks for a proof-of-concept demonstration. We explored magnetic and infrared sensors from Crossbow Technologies to detect some actions that could be used in IED emplacement – emplacement is the step most susceptible to detection – in a public mall and along typical roadside / street environment suggesting potential targets such as government buildings. The threat scenario was emplacement of IEDs in trash receptacles (which could be extended to other public installation such as postal boxes). A network of these sensors was built and positioned in these environments with human subjects entering (some carrying ferromagnetic materials and some not) and proceeding toward a trash receptacle. The sensitivity of the sensors was determined to be less than 50 cm for small objects (electrical circuit board and nails) and two orientations of these sensors were investigated (one of which was more effective than the other).

Experimental results indicated that magnetic sensors were useful in reliably detecting suspicious ferromagnetic materials near and in the trash receptacle (though not all IEDs will contain enough ferrous content to trigger detection). These magnetic sensors, however, were unable to reliably detect small objects, and hence would be ineffective in characterizing ferrous content in a typical packaged IED. Infrared sensors, on the hand, were not as effective in such environments as there is much background infrared radiation.

The objectives set out for the research were satisfactorily achieved. In particular, the experiments showed that magnetic sensors could be used to detect and isolate a receptacle-type IED threat. This suggests that magnetic sensors in a sensor network could be effective for protecting communal areas such as airports and busy urban areas. Other independent technologies such as imagery could be incorporated to build a more robust detection network.

B. FUTURE WORK

Two primary areas are identified for further research:

- Further research is needed in the integration of multiple sensors to improve the decision-making process. In particular, other standoff technologies such as imagery and chemical sensors could be incorporated to improve the selectivity of the thresholds for IEDs, as well as to study the scalability issues associated with such a sensor network.

- Further research should investigate the use of localization such as triangulation methods to determine the threat source. The capability of the sensor network to locate the threat source is just as vital as its detection. A positive localization may minimize unnecessary disruptions like cordoning and crowd dispersal, by confining it to just a particular section instead of the entire building.

APPENDIX A – LISTEN.CLASS CODE

```
package net.tinyos.tools;


import java.sql.*;
import java.io.*;
import java.util.*;
import java.lang.reflect.Array;
import net.tinyos.packet.*;
import net.tinyos.util.*;
import net.tinyos.message.*;
public class Listen {


    private static int moteID;
    private static int PIR;
    private static int mag;
    private static int b1,b2;
    private static String dataSourceName = "background";
    private static String dbURL = "jdbc:odbc:" + dataSourceName;


// To ensure that the right commands are executed
   public static void main(String args[]) throws IOException {
          if (args.length > 0) {
             System.err.println("usage: java net.tinyos.tools.Listen");
             System.exit(2);
          }
```

```
                PacketSource reader = BuildSource.makePacketSource();
        // To check whether there are readings from the serial port.
        if (reader == null) {
System.err.println ("Invalid packet source (check your MOTECOM environment variable)");
                  System.exit(2);
                }

        /*This section opens up the data stream and stores the data packets onto the byte array called
"packet." The modification here is to check whether the reading is a triggered event, which if it is, it will
have a reading of 32 packets. Upon receiving the packets, the mote ID, the magnetic and PIR readings are
calculated to decimal units of measure. */
        try {
         reader.open(PrintStreamMessenger.err);
         for (;;) {
          byte[] packet = reader.readPacket();
                if(Array.getLength(packet) == 32)
                {
                        moteID = Array.getInt(packet,7);
                        b1 = (int)(packet[20]&0xFF);
                        b2 = (int)(packet[21]&0xFF);
                        PIR = b1 + 256*b2;
                        b1 = (int)(packet[22]&0xFF);
                        b2 = (int)(packet[23]&0xFF);
                        mag = b1 + 256*b2;
          System.out.println("Current packet is tracked by Mote : " + moteID);
                  System.out.println("with a PIR of : " + PIR);
                  System.out.println("with a mag of : " + mag);
                  Calendar rightnow = Calendar.getInstance();
                  int hour = rightnow.get(Calendar.HOUR);
                  int min = rightnow.get(Calendar.MINUTE);
                   int sec = rightnow.get(Calendar.SECOND);
           int date = rightnow.get(Calendar.DAY_OF_MONTH);
                   int month = rightnow.get(Calendar.MONTH);
                    int year = rightnow.get(Calendar.YEAR);

                   System.out.println("Detected at " + hour + ":" + min + ":" + sec);
                   System.out.println("Date: " + month + "/" + date + "/" + year);
                    Dump.printPacket(System.out, packet);
                    System.out.println();
                           }

        /* This section deals with the comparison of the readings with the database IED characteristics, by
getting a JDBC-ODBC connectivity first followed by using SQL to compare the values. If the readings
match the values of database, then an alert will be sent out. In this case, the alert is used as a display
statement onto the screen.*/
        try {
               Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
               // set this to a MS Access DB you have on your machine

       Connection con = DriverManager.getConnection(dbURL, "","");
       Statement s = con.createStatement();
       s.execute("select type from mall_environ where mag1 <=" + mag + "and mag2
      >=" + mag);
       ResultSet rs = s.getResultSet();
       if(rs!=null){
        while(rs.next())

        {

                        System.out.println("Possible Type: " + rs.getString(1));

                        }

                        s.close();

                        con.close();

        System.out.println("");

        }


        }

      catch (Exception e) {

      System.out.println("Error: " + e);

  }

          }

        }

        catch (IOException e) {

            System.err.println("Error on " + reader.getName() + ": " + e);
```

APPENDIX B – TEST CASE B DATA

for d = 10cm
Nails
Height 45cm

	5 nails	10 nails	20 nails
Number of Passes	Reading	Reading	Reading
1	534	793	663
2	622	664	745
3	682	657	660
4	644	707	1002
5	508	562	1005
6	510	596	583
7	512	553	1131
8	524	639	1146
9	602	780	993
10	611	783	898
11	509	787	594
12	546	526	626
13	544	654	801
14	531	719	1094
15	509	685	872
16	508	663	1134
17	567	587	762
18	689	685	773
19	522	648	978
20	514	642	1182
	559	**667**	**882**

Height 80cm	5 nails	10 nails	20 Nails
Number of Passes	Reading	Reading	Reading
1	0	588	853
2	626	787	824
3	597	524	888
4	502	731	952
5	611	649	510
6	573	584	869
7	657	786	1130
8	523	697	1171
9	540	512	1068
10	625	762	963
11	0	548	670
12	505	631	1009
13	619	750	944
14	579	544	854
15	584	777	503
16	608	725	930
17	0	501	1036
18	521	742	659
19	532	652	1021
20	556	582	863
	488	**654**	**886**

Ground Level	5 nails	10 nails	20 nails
Number of Passes	Readings	Readings	Reading
1	0	0	0
2	500	0	511
3	510	522	0
4	0	0	523
5	590	512	580
6	0	0	0
7	0	0	0
8	503	523	566
9	0	0	0
10	0	0	0
11	511	562	0
12	0	0	522
13	0	512	0
14	522	0	0
15	510	531	512
16	0	0	562
17	502	526	0
18	0	0	0
19	0	610	0
20	0	0	604
	207	**215**	**219**

for d = 50cm
Nails
Height 45cm

	5 nails	10 nails	20 nails
Number of Passes	Reading	Reading	Reading
1	534	519	622
2	622	643	511
3	701	583	633
4	644	669	587
5	508	539	575
6	510	527	586
7	512	537	621
8	524	675	630
9	602	537	603
10	611	555	679
11	509	682	571
12	546	649	558
13	544	554	547
14	531	658	692
15	509	677	545
16	508	561	539
17	567	650	578
18	689	579	610
19	522	587	674
20	514	547	590
	560	**596**	**598**

Height 80cm	5 nails	10 nails	20 Nails
Number of Passes	Reading	Reading	Reading
1	0	530	580
2	626	657	504
3	597	0	655
4	502	548	676
5	624	550	511
6	573	664	0
7	657	651	649
8	598	544	572
9	540	593	561
10	625	0	694
11	0	698	577
12	505	637	598
13	619	574	572
14	579	697	599
15	584	535	0
16	608	0	582
17	0	620	553
18	521	669	682
19	532	549	593
20	556	512	513
	492	**512**	**534**

Ground Level	5 nails	10 nails	20 nails
Number of Passes	Readings	Readings	Reading
1	0	0	0
2	500	0	0
3	0	622	0
4	0	0	0
5	690	0	690
6	0	0	0
7	0	0	0
8	501	520	731
9	0	0	0
10	0	0	0
11	0	544	0
12	0	0	504
13	0	0	0
14	680	0	0
15	0	631	690
16	0	0	512
17	503	0	0
18	0	0	0
19	0	690	0
20	0	0	550
	144	**150**	**184**

APPENDIX C – TEST CASE C DATA

Circuit Board						
d = 50cm	80cm	45cm	ground	80cm	45cm	ground
Number of Passes	Reading	Reading	Reading	**d = 10cm**		
1	744	508	0	770	543	0
2	680	568	534	767	522	567
3	666	554	610	763	562	673
4	765	661	0	784	765	558
5	651	585	0	789	732	671
6	670	640	553	831	620	553
7	653	556	0	675	534	0
8	531	606	0	688	539	577
9	583	548	0	697	598	0
10	621	503	610	703	603	0
11	511	638	534	781	702	621
12	706	694	0	693	579	0
13	507	595	0	621	560	0
14	511	512	521	665	574	577
15	527	506	556	553	588	0
16	548	603	0	579	602	0
17	657	557	0	563	533	560
18	501	583	501	559	537	521
19	776	550	0	590	542	0
20	579	596	0	534	549	0
	619	**578**	**221**	**680**	**589**	**294**

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D – TEST CASE D DATA

Test D outside mote height=0cm, t=0.2cm

Id	Sample #	pir	mag
6	5	969	0
1	8	701	0
1	9	991	0
6	6	1023	0
6	7	1023	0
6	8	1023	0
6	9	1023	0
6	10	1023	0
1	10	682	0
6	11	741	0
6	12	759	0
1	11	991	0
6	13	778	0
1	12	693	501
6	14	1023	0
6	15	1023	0
6	16	719	0
1	13	1023	0
1	14	1023	0
6	17	1023	0
6	37	951	0
6	38	1023	0
1	26	953	0
1	27	1023	529
6	39	1023	0
6	40	1023	0
6	41	919	511
6	42	919	503
6	43	1023	508
1	30	985	0
6	44	830	0
1	31	0	512
6	45	1023	0
6	46	649	0
1	36	1017	0
1	37	1017	507
6	47	1023	0
6	48	905	0
6	49	1023	0
1	38	645	503
6	50	1023	0
1	39	0	507
1	40	1023	507
6	51	1023	0
1	41	597	509

Test D outside mote height=90cm, t=0.2cm

Id	Sample #	pir	mag
1	145	1023	515
6	227	1023	529
1	146	1023	515
6	229	1023	514
6	231	918	502
1	147	665	526
1	148	1023	526
6	232	1023	502
6	234	910	0
1	149	727	515
6	235	910	504
1	150	1023	515
6	236	1023	504
6	239	875	518
1	155	1023	525
6	241	1023	515
1	156	1023	525
6	244	973	503
1	158	610	522
6	245	973	503
1	159	1023	522
6	246	973	513
6	247	1023	513
1	164	662	520
1	165	1023	520
6	253	979	511
1	167	682	514
6	254	1023	508
6	255	1023	508
1	168	1023	514
1	169	1023	975
6	256	1023	531
6	257	1023	531
1	170	821	503
6	258	1023	516
1	171	821	503
6	262	862	505
1	175	1023	531
1	176	609	520
6	266	860	515
1	177	1023	520
6	267	943	515
6	269	1023	539
1	178	639	515
6	270	1023	564

6	52	930	0
1	42	1023	509
6	53	1023	0
1	44	602	510
6	54	1023	0
1	45	612	513
1	46	1023	513
6	55	1023	0
6	56	1023	0
6	57	1023	0
6	58	1023	0
Node inside dustbin			509
Node outside dustbin			0

Test D outside mote height=45cm, t=0.2cm

Id	Sample #	pir	mag
1	64	1023	504
6	89	1023	511
1	65	1023	504
6	90	1023	521
6	91	1023	521
1	66	633	513
6	92	1023	503
6	93	1023	503
1	67	642	512
6	96	847	503
6	97	1023	503
6	99	1023	0
1	69	630	518
6	100	1023	504
1	70	1023	518
1	71	954	502
6	103	1023	504
1	72	1023	502
6	104	1023	504
1	73	999	525
6	107	1023	503
1	74	1023	525
6	108	1023	503
1	76	660	515
1	77	1023	515
6	111	1023	507
6	112	1023	507
1	78	653	504
1	79	1023	504
6	114	1023	581
1	81	1023	563
1	82	1023	563
6	117	1023	507
1	83	613	504
6	121	1023	504
1	84	1023	504
Node inside dustbin			516
Node outside dustbin			483

1	179	1023	515
6	271	1023	564
Node inside dustbin			539
Node outside dustbin			497

SUDDEN EMPLACEMENT

1	74	1023	514
1	75	1023	1392
1	76	1023	1392
1	77	1023	793
1	78	1023	793
1	79	1023	608
1	80	836	747
1	81	848	502
1	82	1023	883
1	83	1023	857
1	84	898	864
1	85	1023	512
1	86	1023	1221
1	87	1023	1088
1	88	799	655
1	89	663	569
1	90	1023	569
1	91	1023	1332
1	92	1023	3349
1	93	904	996
1	94	904	578
1	95	634	1255
1	96	1023	1255
1	97	1023	1605
1	98	881	1605
1	99	1023	976
1	100	931	866
1	105	944	789
1	106	918	923
1	107	1023	944
1	108	914	868
1	111	785	754
1	112	1023	813
1	113	1023	602
			819

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Bruce Hoffman, “The Logic of Suicide Terrorism,” in Terrorism and Counterterrorism: Understanding the New Security Environment. McGraw Hill, 2004.

[2] B. Raman, “Suicide & Suicidal Terrorism,” South Asia Analysis Group Paper No. 947. Mar 2004. Available from http://www.fas.org/irp/threat/terrorism/sup3.pdf, last accessed 9 Aug 2007.

[3] CRS Report for Congress – “Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures.” Sep 2006. Available from http://research.fit.edu/fip/documents/SecNews1.pdf, last accessed 9 Aug 2007.

[4] David W. Hannum, “Survey of Commercially Available Explosives Detection Technologies and Equipment,” Sandia National Laboratories. Sep 1998. Available from http://www.ncjrs.gov/pdffiles1/nij/grants/208861.pdf, last accessed 10 Sep 2007.

[5] DoD Directive 2000.19E, "Joint Improvised Explosive Device Defeat Organization (JIEDDO),” February 14, 2006. Available from http://www.dtic.mil/whs/directives/corres/pdf/200019p.pdf, last accessed 9 Aug 2007.

[6] DCSINT Handbook No. 1.03, “Suicide Bombing.” Aug 2005. Available from http://stinet.dtic.mil/cgibin/GetTRDoc?AD=ADA439887&Location=U2&doc=GetTRDoc.pdf, last accessed 10 Aug 2007.

[7] Defense News, “The IED Marketplace in Iraq.” August 3rd, 2005. Available from http://globalguerrillas.typepad.com/globalguerrillas/2005/08/the_ied_marketp.html, last accessed 15 Oct 2007.

[8] Department of Homeland Defense, “The Support Anti-terrorism by Fostering Effective Technologies Act of 2002.” Available from http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm, last accessed 11 Oct 2007.

[9] E. Cayirci, et al., “Wireless sensor networks: a survey.” *IEEE Computer*, vol. 38, no. 4, pages 393-422. Mar 2002. Available from http://www.ece.gatech.edu/research/labs/bwn/sensornets.pdf, last accessed 23 Aug 2007.

[10] FM 5-250, “Explosives and Demolition.” Jun 1992. United States Army. Available from http://www.preterhuman.net/texts/terrorism_and_pyrotechnics/explosives/MISC/Explosives%20and%20Demolitions%20-%20FM%205-250.pdf, last accessed 29 Oct 2007.

[11] FM 3-34.119/MCIP 3-17.01, “Improvised Explosive Defeat.” Sep 2005. United States Army. Excerpt available from http://www.fas.org/irp/doddir/army/fmi3-34-119-excerpt.pdf, last accessed 30 Oct 2007.

[12] Greg Grant, “US Begins to Counter IED Threat,” *Jane's Defense Weekly*. Mar 2005. Available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml, last accessed 11 Aug 2007.

[13] GTA 90-01-001, “Improvised Explosive Device (IED) and Vehicular Borne Improvised Explosive Device (VBIED) Smart Card.” Available from www.wood.army.mil/cehc/Resources.htm, last accessed 11 Aug 2007.

[14] Google Image Search. Available from www.images.google.com, last accessed 1 Sep 2007.

[15] Global Security. Available from www.globalsecurity.org, last accessed 13 Sep 2007.

[16] Iraq Coalition Casualty Count. Available from www.icasualties.org, last accessed 1 Sep 2007.

[17] James I. Rostberg, “Common Chemicals as Precursors of Improvised Explosive Devices: The Challenges of Defeating Domestic Terrorism,” Masters Thesis, Naval Postgraduate School. Sep 2005. Available from http://www.terrorisminfo.mipt.org/pdf/NPS-Thesis-Common-Chemicals-Precursors.pdf, last accessed 5 Sep 2007.

[18] John P. Sullivan, et al., “Jane's Unconventional Weapons Response Handbook.” 2002. Available from http://www.au.af.mil/au/awc/awcgate/army/guidterr/app_e.pdf, last accessed 13 Aug 2007.

[19] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, “System Architecture Directions for Networked Sensors,” ASPLOS. Nov 2000. Available from www.tinyos.net/papers/tos.pdf, last accessed 22 Sep 2007.

[20] John A. Stankovic, “Research Challenges for Wireless Sensor Networks.” Available from www.cs.virginia.edu/sigbed/archives/stankovic.pdf, last accessed 7 Sep 2007.

[21] Judee Burgoon, et al., “Workshop Report on Detecting and Countering IEDs and Related Threats,” NSF IED Workshop. Jun 2006. Available from http://www.tinyos.net/papers/tos.pdf, last accessed 4 Aug 2007.

[22] Joint Publication 3-06, “Doctrine for Joint Operations.” Sep 2002. Available from http://www.nytimes.com/package/pdf/international/021021dod_report.pdf, last accessed 14 Aug 2007.

[23] M. Haenggi, “Opportunities and Challenges in Wireless Sensor Networks.” 2005. In M. Ilyas and I. Mahgoub, editors, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press. Available from http://doc.romeo.org.ua/Sl.G.Gubar/BOOKS/elecronix/Handbook%20of%20Sensor%20Networks%20Compact%20Wireless%20and%20Wired/1968_C01.pdf, last accessed 29 Oct 2007.

[24] Michael J. Caruso & S. Lucky, “Vehicle Detection and Compass Applications using Magnetic Sensors,” Honeywell Inc. Available from http://www.magneticsensors.com/datasheets/am.pdf, last accessed 15 Sep 2007.

[25] MSP410 User Manual. Available from www.crossbow.com, last accessed 8 Oct 2007.

[26] MSNBC, “*U.S. Spending Billions to ‘Defeat’ IEDs in Iraq*,” 13 Mar 2006. Available from www.msnbc.msn.com/id/11813982/print/1/displaymode/1098/, last accessed 10 Aug 2007.

[27] N. Xu, “A Survey of Sensor Network Applications.” Available from http://enl.usc.edu/»ningxu/papers/survey.pdf, last accessed 7 Oct 2007.

[28] Nomadics Inc., Final technical report “Explosive Chemical Signature-Based Detection of IEDs.” Dec 2004. Available from http://stinet.dtic.mil/cgi-bin/GetTRDocAD=ADA430111&Location=U2&doc=GetTRDoc.pdf, last accessed 6 July 2007.

[29] National Science Foundation, Award # 0731102. Sep 2007. Abstract available from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0731102, last accessed 22 Oct 2007.

[30] Philip E. Colon et al., “Modeling Human Perception of Situation Awareness During Constructive Experimentation.” 2007. Available from www.isi.edu/~ddavis/JESPP/2007_Papers/TranCurielYao&Anhalt/7748.pdf, last accessed 3 Oct 2007.

[31] Ryan Miller, “Power Management for Mica2 Motes.” Department of Computer Science, North Carolina State University. Available from www.cs.etsu.edu/sasplas/papers/davis-miller%20paper.doc, last accessed 30 Oct 2007.

[32] Shnayder V. et al., "Simulating the Power Consumption of Large Scale Sensor Network Applications." In *SenSys '04*. 2004. Available from www.eecs.harvard.edu/~shnayder/papers/sensys04ptossim.pdf, last accessed 30 Oct 2007.

[33] The Aluminum Association, Inc. Available from www.aluminium.org, last accessed 4 Oct 2007.

[34] Trammell Hike, et al., "Using unmanned aerial vehicle-borne magnetic sensors to detect and locate improvised explosive devices and unexploded ordnance," Proceedings of the SPIE, Volume 5778, 2005. Available from http://adsabs.harvard.edu/abs/2005SPIE.5778.963T, last accessed 14 Aug 2007.

[35] Transportation Security Administration, "Federal Efforts for Rail and Surface Transportation Security." Jan 2007. Available from www.tsa.gov/assets/pdf/testimony_senate_rail_1.18.07.pdf, 5 Oct 2007.

[36] United States Environmental Protection Agency, "Municipal Solid Waste Generation, Recycling, and Disposal in the United States: Facts and Figures 2005." Available from www.epa.gov/msw/pubs/mswchar05.pdf, last accessed 5 Oct 2007.

[37] Vlasios Salatas, "Object Tracking Using Wireless Sensor Networks," Masters Thesis, Naval Postgraduate School. Sep 2005. Available from http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439599&Location=U2&doc=GetTRDoc.pdf, last accessed 25 Aug 2007.

[38] XyTrans Inc., "Longer Stand-off Distance for IED Detection." Jul 2006. Available from www.xytrans.com/pdf/IED%20Detection%20White%20Paper.pdf, last accessed 8 Sep 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Peter J. Denning
   Chair, Department of Computer Science
   Naval Postgraduate School
   Monterey, California

4. Professor Gurminder Singh
   Director, Center for the Study of Mobile Devices and Communications
   Naval Postgraduate School
   Monterey, California

5. Professor Neil C. Rowe
   Chair, Autonomous Systems Track, Department of Computer Science
   Naval Postgraduate School
   Monterey, California